TP-LINK®

24+4G 千兆二层全网管交换机

TL-SL5428

用户手册

Rev: 2.1.0
1910040221

声明

本手册所提到的产品规格和资讯仅供参考，如有内容更新，恕不另行通知。可随时查阅我们的万维网页。除非有特殊约定，本手册仅作为使用指导，本手册中的所有陈述、信息等均不构成任何形式的担保。

目录

第1章 用户手册简介

本手册旨在帮助您正确使用这款交换机。手册中包括对交换机性能特征的描述以及配置交换机的详细说明。请在操作交换机前，详细阅读本手册。

1.1 目标读者

本手册的目标读者为熟悉网络基础知识、了解网络术语的技术人员。

1.2 本书约定

在本手册中，

- 所提到的“交换机”、“本产品”等名词，如无特别说明，系指 TL-SL5428 24+4G 千兆二层全网管交换机，下面简称为 TL-SL5428。
- 用 **>>** 符号表示配置页面的进入顺序。默认为**一级菜单 >> 二级菜单 >> 标签页**。
- 正文中出现的<>尖括号标记的文字，表示 Web 页面的按钮名称，如<确定>。
- 正文中出现的**加粗**标记的文字，表示交换机的各个功能的名称，如**端口配置**页面。
- 正文中出现的“”双引号标记的文字，表示配置页面上出现的名词，如“IP 地址”。

本手册中使用的特殊图标说明如下：

图标	含义
注意：	该图标提醒您对设备的某些功能设置引起注意，如果设置错误可能导致数据丢失，设备损坏等不良后果。
说明：	该图标表示此部分内容是对相应设置、步骤的补充说明。

1.3 章节安排

章节	章节说明
第 1 章 用户手册简介	帮助您快速掌握本手册的结构、了解本手册的约定，从而更有效地使用本手册。
第 2 章 产品介绍	介绍本产品的特性、应用以及外观。

章节	章节说明
第 3 章 配置指南	介绍如何登录 TL-SL5428 的 Web 页面，并简要介绍页面特点。
第 4 章 系统管理	本模块主要用于配置交换机的系统属性，主要介绍了： ● 系统信息：配置交换机的描述、时间和网络参数。 ● 用户管理：配置登录交换机 Web 页面的用户的访问权限和身份。 ● 系统工具：集中对交换机的配置文件进行管理。 ● 安全管理：安全管理：针对不同的登录方式，增强用户管理交换机的安全性。包括安全配置、SSL 配置和 SSH 配置。
第 5 章 二层交换	本模块主要用于配置交换机的基本功能，主要介绍了： ● 端口管理：配置交换机端口的基本属性包括端口配置、端口镜像、端口安全和端口隔离。 ● 汇聚管理：配置端口汇聚组。汇聚是将交换机的多个物理端口聚合在一起形成一个逻辑端口，同一汇聚组内的多条链路可视为一条逻辑链路。 ● 流量统计：统计流经各个端口的数据信息。 ● 地址表管理：配置交换机的地址表。地址表是交换机实现报文快速转发的基础。
第 6 章 VLAN	VLAN 主要用于隔离广播域，通过划分虚拟工作中来简化网络管理，主要介绍了： ● 802.1Q VLAN：划分基于端口的 VLAN，也是 MAC VLAN 和协议 VLAN 的基础。 ● MAC VLAN：在不改变原 802.1Q VLAN 配置的情况下划分 MAC VLAN。 ● 协议 VLAN：从应用层划分 VLAN，使某些特殊网络数据只能在指定 VLAN 中传输。 ● GVRP：通过在端口动态注册和注销 VLAN 信息来达到配置 VLAN 的目的，并传播 VLAN 信息到其它交换机中，简化配置 VLAN 时的操作。 ● VLAN VPN：通过 VLAN 映射将私网报文的 VLAN Tag 映射到公网 VLAN Tag，并在公网 VLAN 传输报文。 ● Private VLAN：通过建立 Private VLAN，上层设备只需识别少量的 primary VLAN，从而节省上层设备的 VLAN 资源。
第 7 章 生成树	生成树主要用于在局域网中消除环路。本模块主要用于配置交换机的生成树功能，主要介绍了： ● 基本配置：配置和查看交换机生成树功能的全局属性。 ● 端口配置：配置端口的 CIST 参数。 ● MSTP 实例：配置 MSTP 实例。 ● 安全配置：配置保护功能，以防止生成树网络中的设备遭受恶意攻击。

章节	章节说明
第 8 章 组播管理	本模块主要用于配置交换机的组播管理功能，主要介绍了： ● IGMP 侦听：配置 IGMP 侦听的全局参数、端口属性、VLAN 参数和组播 VLAN。IGMP 侦听可以有效抑制组播数据在网络中扩散。 ● 组播地址表：配置组播地址表。交换机在转发组播数据时是根据组播地址表来进行的。 ● 组播过滤：配置组播过滤功能，可以限制用户对组播节目的点播。 ● 报文统计：查看各端口的组播报文流量，帮助您监控网络中 IGMP 报文。
第 9 章 服务质量	本模块主要为网络中某些特殊应用程序提供保障，主要介绍了： ● QoS 配置：给网络中的数据流划分优先级，保障重要数据的传输，可分为端口优先级、802.1P 优先级和 DSCP 优先级。 ● 流量管理：可通过带宽控制来限制端口的数据流量；风暴抑制可限制局域网中各类广播包的传输带宽，节约网络资源。 ● 语音 VLAN：在指定 VLAN 中传输语音数据，提高语音数据的传输优先级，保证通话质量。
第 10 章 访问控制	本模块通过配置对报文的匹配规则和处理操作来实现对数据包的过滤功能，有效防止非法用户对网络的访问，节约网络资源，主要介绍了： ● 时间段配置：通过时间段控制 ACL 条目的生效时间。 ● ACL 配置：配置 ACL 条目。 ● Policy 配置：配置 ACL 规则的处理方式。 ● 绑定配置：将 Policy 下发到端口和 VLAN，使之正式生效。
第 11 章 网络安全	本模块针对局域网中常见的网络攻击进行防护，主要介绍了： ● 四元绑定：是将计算机的 MAC 地址和 IP 地址，所属 VLAN 以及连接交换机的端口号四者绑定。 ● ARP 防护：对局域网中的 ARP 攻击进行防护。 ● IP 源防护：对局域网中的 IP 数据包进行过滤。 ● DoS 防护：对常见的 DoS 攻击进行防护。 ● 802.1X 认证：配置交换机对局域网接入用户进行接入认证。
第 12 章 SNMP	SNMP 提供了一个管理框架来监控和维护互联网设备。本模块主要用于配置交换机的 SNMP 功能，主要介绍了： ● SNMP 配置：配置 SNMP 的基本属性。 ● 通知管理：配置 SNMP 通知管理，便于管理软件对交换机某些事件进行及时监控和处理。 ● RMON：配置 RMON 功能，便于网管更有效的监控网络。
第 13 章 集群管理	集群管理的主要目的是解决大量分散的网络设备的集中管理问题。模块主要用于配置交换机的集群管理功能，主要介绍了： ● 拓扑发现：配置拓扑发现功能。用于获取与其直接相连的邻居交换机的信息。 ● 拓扑收集：配置拓扑收集功能。用于命令交换机收集网络的拓扑信息。 ● 集群管理：配置集群管理功能。用于建立和维护集群。

章节	章节说明
第 14 章 系统维护	系统维护模块将管理交换机的常用系统工具组合在一起，主要介绍了： ● 运行状态：对交换机内存和 CPU 进行监控。 ● 系统日志：查看在交换机上配置的参数。 ● 线缆检测：检测与交换机连接的线缆是否有故障。 ● 环回检测：检测交换机与对端设备的可用性。 ● 网络诊断：检测目标是否可达以及目标与交换机之间的路由跳数。
第 15 章 软件系统维护	主要介绍了：当交换机出现软件故障时，如何进入交换机的 boot 菜单重新加载软件。
附录A 802.1X客户端软件使用说明	主要介绍了如何使用我司提供的 802.1X 客户端软件，并利用该软件进行认证。
附录B 术语表	整理用户手册中出现的术语。
附录C 技术参数规格	技术参数规格表。

回目录

第2章 产品介绍

2.1 产品简介

TL-SL5428 交换机是一款由深圳市普联技术有限公司自主设计和开发的，为构建高安全、高性能网络需求而专门设计的新一代二层全网管交换机，具有 4GE 上行、完备的安全策略、完善的 QoS 策略、丰富的 VLAN 特性、易管理维护等特点。系统采用全新的软硬件平台，在安全接入策略、多业务支持、易管理和维护等方面为用户提供了全新的技术特性和解决方案，是理想的办公网、校园网的汇聚、接入层交换机以及中小企业、分支机构的核心交换机。

2.2 产品特性

完备的网络接入安全策略

- 一键快速绑定

支持 PORT/MAC/IP/VLAN ID 四元绑定，提供手动添加、自动扫描、DHCP 侦听三种绑定方式，支持跨 VLAN 扫描，根据不同网络环境，轻松实现快速绑定。

- ARP 攻击防护

内置特有的 ARP 入侵检测功能，对不匹配四元绑定表的非法 ARP 欺骗报文直接丢弃，有效杜绝内网 ARP 攻击；支持对非法 ARP 报文统计，帮助用户迅速定位 ARP 攻击源；同时还支持防合法 ARP 报文的泛滥攻击。

- IP 源防护

利用在交换机中绑定的四元信息对 IP 包进行检查，过滤不符合四元绑定表的 IP 报文，只处理与四元绑定表吻合的数据包，提高交换机带宽资源的利用率。

- DoS 攻击防护

内置深层次攻击检测功能，通过解析 IP 数据包，查看数据包中的特定字段是否符合 DoS 攻击数据包的特征，并采取相应的防护措施，直接丢弃非法数据包或者对合法的数据包进行限速，并且还能主动探测追踪 DoS 攻击的源头。

- 防 MAC 地址攻击

支持端口安全特性，可以有效防御 MAC 地址攻击。可以实现基于 MAC 地址允许或限制流量，每个端口允许设定最大 MAC 地址数量，支持静态配置或交换机动态学习，全面保障网络安全。

多层次，多元化的访问控制策略

- 访问控制（ACL）

强大硬件 ACL 能力，深度识别报文，支持 L2~L4 数据流分类，提供基于源 MAC 地址、目的 MAC、源 IP 地址、目的 IP 地址、IP 协议类型、TCP/UDP 端口等定义 ACL。

- 策略控制（policy）

支持基于端口、VLAN 下发 ACL，对符合相应 ACL 规则的数据包实现流分类，可进行流镜像、流监控、QoS 重标记和端口重定向四种行为控制，轻松实现网络监控，数据流量控制，优先级重标记和数据转发控制。

- 时间段控制

新增基于时间段的 ACL 控制，提供节假日、绝对时间、周期以及时间片段设置功能，多种时间段的灵活组合可轻松实现对时间精确控制的访问需求。

- 802.1X 认证

支持基于端口和基于 MAC 的 802.1X 认证，在用户接入网络时完成必要的身份认证，保证接入用户的合法性，支持 Guest VLAN，轻松设置来宾用户接入访问权限。

丰富的 VLAN 特性

- IEEE 802.1Q VLAN

IEEE 802.1Q VLAN 符合国际标准，完美融合了 Port VLAN，与主流设备完全兼容，加上人性化的操作方式，使组网更加便捷、准确、高效。

- MAC VLAN

通过 MAC 地址划分 VLAN，使用户可以灵活更改接入位置而不必重新划分 VLAN，在极大提高组网的灵活性的同时，简化了网络拓扑结构和配置管理。

- 协议 VLAN

通过协议来划分 VLAN，对特殊应用可设置自定义协议，实现安全通信。

- VLAN VPN（QinQ），VLAN 映射

有效扩展 VLAN 资源，实现用户 VLAN 的透传技术，便于在智能小区、企业网或园区网中组建多层交换网络。

- GVRP

基于 GARP 的工作机制，用来维护设备中的 VLAN 动态注册信息，使得局域网内的 VLAN 配置更快捷、方便。

完善多业务融合能力

- QoS

支持基于端口、IEEE802.1p 以及 DSCP 三种优先级模式，支持 Equ、SP（Strict priority）、WRR（Weighted Round Robin）、SP+WRR 四种队列调度算法，每个端口 4 个输出队列，可以将不同优先级的报文映射到不同输出队列，保障关键业务数据优先处理，满足不同业务对基础网络的需求。

- 流量控制

带宽控制支持端口双向限速，限速的控制粒度为 100Kbps；风暴抑制支持对广播包、组播包、UL 包限速，避免网络资源被恶意浪费，提高网络效率。

- 语音 VLAN

内置语音设备 OUI 地址识别功能，通过 Voice VLAN 技术，对语音流进行有针对性的 QoS 配置，能够很好的解决语音设备数据流优先级的调整问题，保证通话质量。

- 组播管理

支持 IGMPV1/V2/V3，通过 IGMP Snooping 技术，能很好的解决组播应用，如 IPTV、视频会议等等；支持组播 VLAN，有效避免带宽浪费，减轻上游设备的组播负担；静态组播地址表减少学习时间，提高组播转发效率；未知组播报文丢弃功能，节省带宽，提高系统处理效率。

高可靠性设计

- 生成树

支持传统的 STP/RSTP/MSTP 二层链路保护技术，极大提高链路的容错、冗余备份能力，保证网络的稳定运行。支持 TC（Topology Change）报文保护，避免当设备受到恶意的 TC 报文攻击时，频繁的删除操作给设备带来很大负担。同时还支持环路保护、根桥保护、BPDU 保护、BPDU 过滤等功能。

- 链路汇聚

提供手工汇聚、静态 LACP、动态 LACP 三种汇聚模式，能有效增加链路带宽，提高链路的可靠性，同时可以实现负载均衡、链路备份。

灵活、安全的网络管理

- 系统管理

支持 CLI 命令行（Console，Telnet，SSHV1/V2 ），Web 网管（http、SSL V2/V3/TLSV1），SNMP（V1/V2c/V3）等多种管理方式。

- 安全管理

通过身份过滤检测技术，能够很好的解决设备安全管理难题，支持两级用户管理，提供管理人员数限制功能，增强配置安全性。

- 网络监控

支持端口双向数据监控，结合网络分析软件可以实时监控网络运行状态，RMON 功能可以实现统计和告警功能，用于网络中管理设备对被管理设备的远程监控和管理。

- 系统维护

支持 CPU、内存实时监控，支持 VCT 电缆检查以及端口环回测试，方便定位网络故障点，同时支持 Ping、Tracert 命令操作，轻松分析出现故障的网络节点。

- 系统日志

提供免费的日志服务器软件，为用户提供对设备系统日志的数据库统计分析功能，有效监控设备运行和网络状况。

- 集群管理

支持 NDP(邻居发现)、NTDP（邻居拓扑发现）和 Web 集群管理，轻松打造“零费用、免软件”的统一管理方式，支持信息产业部相关标准，兼容其它主流厂商的集群管理。

2.3 产品外观

2.3.1 前面板

24+4G千兆网管交换机的前面板由 24 个 10/100M端口、4 个 1000M端口、2 个SFP口、1 个Console口和指示灯组成，如图 2-1所示。

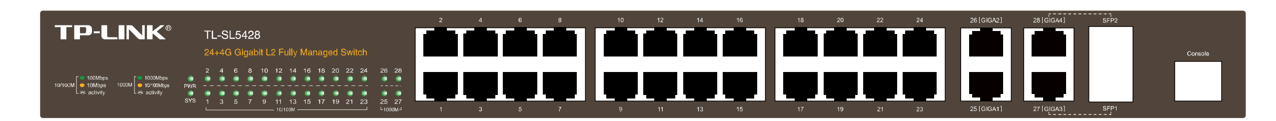


图 2-1 前面板

➢ **24 个 10/100Mbps 自适应 RJ45 端口**

本系列交换机的 1-24 端口均支持 10Mbps/100Mbps 带宽的连接设备的端口。每个端口对应一个 10/100M 指示灯。

➢ **4 个 10/100/1000Mbps 自适应 RJ45 端口**

本系列交换机的 25-28 端口均支持 10Mbps/100Mbps/1000Mbps 带宽的连接设备的端口。每个端口对应一个 1000M 指示灯。

➢ **2 个 SFP 端口**

SFP 模块卡扩展槽位于千兆 RJ45 端口的右边，同与其 Combo 共享的千兆 RJ45 端口共用指示灯，其中 SFP1 与端口 27 共用，SFP2 与端口 28 共用。

➢ **1 个 Console 端口**

Console 端口位于面板的最右边。

➢ 指示灯

指示灯，包括 PWR，SYS，10/100M，1000M 指示灯。通过指示灯您可以监控交换机的工作状态，下表将详细说明指示灯工作状态：

指示灯	名称	状态	描述
PWR	电源指示灯	常亮	系统供电正常
		闪烁	系统供电异常
		熄灭	系统未通电或供电异常
SYS	系统指示灯	常亮	系统出现异常
		闪烁	系统正常工作
		熄灭	系统出现异常
10/100M	端口指示灯	常亮	端口已正常连接
		闪烁	端口正在传输数据
		绿色	端口速率为 100Mbps
		黄色	端口速率为 10Mbps
1000M	端口指示灯	常亮	端口已正常连接
		闪烁	端口正在传输数据
		绿色	端口速率为 1000Mbps
		黄色	端口速率为 100Mbps 或 10Mbps

2.3.2 后面板

交换机后面板由电源接口和防雷接地柱组成，如图 2-2所示：

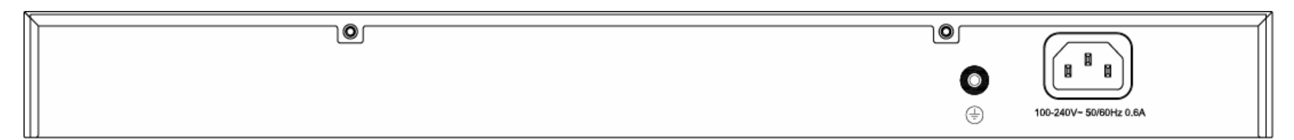


图 2-2 后面板

➢ **电源接口**

位于后面板右侧，接入电源需为 100-240V~ 50/60Hz 0.6A 的交流电源。

➢ **防雷接地柱**

位于电源接口左侧，请使用导线接地，以防雷击。

 注意：

- 请使用原装电源线。
- 电源插座请安装在设备附近便于触及的位置，以方便操作。

回目录

第3章 配置指南

3.1 登录Web页面

第一次登录时，请确认以下几点：

1) 交换机已正常加电启动，任一端口已与管理主机相连。

2) 管理主机已正确安装有线网卡及该网卡的驱动程序、并已正确安装 IE 6.0 或以上版本的浏览器。

3) 管理主机 IP 地址已设为与交换机端口同一网段，即 192.168.0.X（X 为 2 至 254 之间的任意整数），子网掩码为 255.255.255.0。

4) 为保证您更好地体验 Web 页面显示效果，建议您将显示器的分辨率调整到 1024×768 或以上像素。

打开IE浏览器，在地址栏输入http://192.168.0.1 登录交换机的Web页面。



交换机登录页面如图 3-1所示。



图 3-1 登录页面

在此页面输入交换机管理帐号的用户名和密码，出厂默认值为admin/admin。成功登录后可以看到交换机的系统信息，如图 3-2所示。

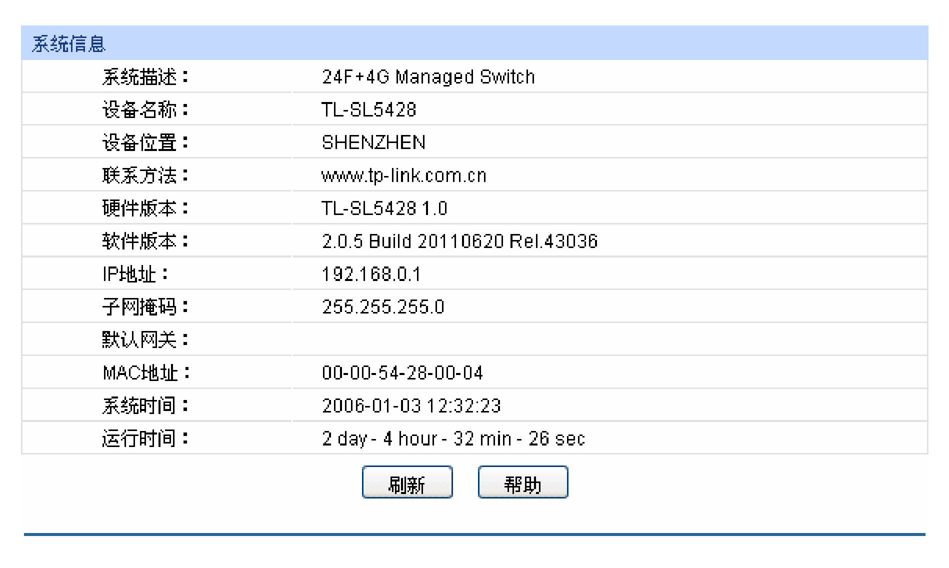


图 3-2 系统信息

3.2 Web页面简介

3.2.1 页面总览

交换机典型的Web页面如图 3-3所示。



图 3-3 典型 Web 页面

在图 3-4中可以看到，左侧为一级、二级菜单栏，右侧上方长条区域为菜单下的标签页，当一个菜单包含多个标签页时，您可以通过点击标签页的标题在同级菜单下切换标签页。右侧标签页下方区域可分为三部分，条目配置区、列表管理区以及提示和注意区。



图 3-4 Web 页面区域划分

3.2.2 页面常见按键及操作

➢ 主菜单区按键

按键	含义
配置保存	保存最终的配置。
退出登录	退出 Web 页面。

注意:

● 配置交换机后，点击<提交>按键当前配置立即生效，但重启后参数将失效；若需要当前配置在交换机重启后依旧生效，则需要点击<配置保存>按钮，建议在交换机断电或重启前<配置保存>。

➢ 条目配置区常见按键

按键	含义
提交	提交当前的配置。
添加	添加当前配置条目。
修改	修改并保存编辑后的配置信息。
清空	快速清空当前配置项中已输入的所有信息。
帮助	打开当前功能的帮助页面。



说明：

- <修改>按键只有在编辑列表中的条目时才会出现，取代原本的<新增>按键。

➢ 列表管理区常见按键

按键	含义
全选	选中当前列表中所有条目。
删除	删除选中的条目，可批量操作。
刷新	刷新列表。
选择	根据所输序号，快速选择至列表中的对应条目。

回目录

第4章 系统管理

系统管理模块主要用于配置交换机的系统属性，包括**系统配置**、**用户管理**、**系统工具**以及**安全管理**四个部分。

4.1 系统配置

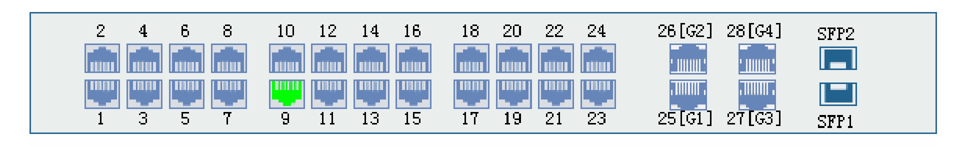
系统配置用于配置交换机的基本属性，本功能包括**系统信息**、**系统描述**、**系统时间**和**管理 IP** 四个配置页面。

4.1.1 系统信息

本页面用来查看本交换机的端口连接信息和系统信息。

端口状态界面指示了本交换机的 24 个 10/100Mbps RJ45 端口、4 个 10/100/1000Mbps RJ45 端口以及 2 个 SFP 扩展模块槽的工作状态，其中以数字标识的端口是 10/100Mbps RJ45 端口，标识为 G 的端口 10/100/1000Mbps RJ45 端口，标识为 SFP 的端口是光纤模块端口。

进入页面的方法：系统管理>>系统配置>>系统信息



系统信息	
系统描述：	24F+4G Managed Switch
设备名称：	TL-SL5428
设备位置：	SHENZHEN
联系方法：	www.tp-link.com.cn
硬件版本：	TL-SL5428 1.0
软件版本：	2.0.5 Build 20110620 Rel.43036
IP地址：	192.168.0.1
子网掩码：	255.255.255.0
默认网关：	
MAC地址：	00-00-54-28-00-04
系统时间：	2006-01-03 12:32:23
运行时间：	2 day - 4 hour - 32 min - 26 sec

刷新 帮助

图 4-1 系统信息

条目介绍：

- **端口状态**

100M 端口未接入设备。

100M 端口工作速率为 100Mbps。

100M 端口工作速率为 10Mbps。



1000M 端口未接入设备。

1000M 端口工作速率为 1000Mbps。

1000M 端口工作速率为 100 Mbps /10Mbps。

SFP 端口未接入设备。

SFP 端口工作速率为 1000Mbps。

SFP 端口工作速率为 100Mbps。

当鼠标移到某端口上时，会显示该端口的详细信息，如下图所示。

端口：6
类型：100M RJ45
速率： 100M, 全双工
状态： 已连接, 启用

图 4-2 端口信息

条目介绍：

➢ 端口信息

端口： 显示交换机的端口号。

类型： 显示端口的端口类型。

速率 显示端口的最大传输速率。

状态： 现在端口的状态。

点击某端口，会显示此端口的带宽利用率，即实际传输速率与其最大传输速率的百分比，图中每隔 4 秒反馈一次监控值。查看各个端口的带宽利用率，可以帮助您及时了解各端口的流量概况，便于监控网络流量和分析网络异常。如下图所示。

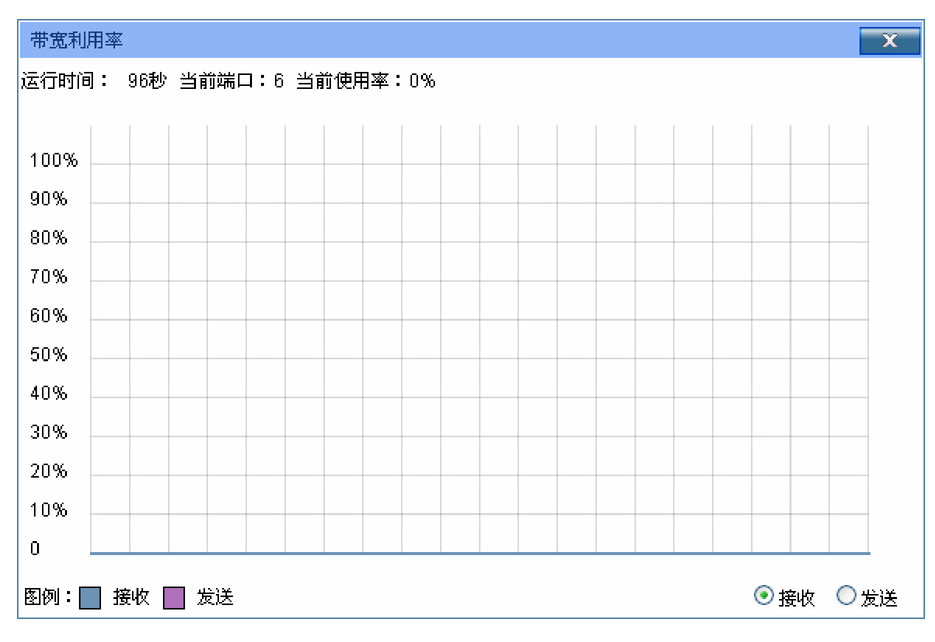


图 4-3 带宽利用率

条目介绍：

➢ 带宽利用率

接收	点击后，显示此端口接收数据的带宽利用率。
发送	点击后，显示此端口发送数据的带宽利用率。

4.1.2 设备描述

本页面用来配置交换机的描述信息，包括设备名称、设备位置、联系方法。

进入页面的方法：系统管理>>系统配置>>设备描述

设备描述

设备名称： TL-SL5428

设备位置： SHENZHEN

联系方法： www.tp-link.com.cn

提交

注意：

设备名称、设备位置和联系方法最长可输入32个字符。

图 4-4 系统描述

条目介绍：

➢ 设备描述

设备名称：	填写交换机的名称。
设备位置：	填写交换机的位置信息。
联系方法：	填写您的联系方法。

4.1.3 系统时间

本页面用来配置交换机的系统时间。系统时间是交换机工作时使用的时间，其它功能（如访问控制）中的时间信息以此处为准。可以选择手动设置时间或者连接到一个 NTP(网络时间协议)服务器获取 GMT 时间，也可以获取当前管理 PC 的时间作为交换机的系统时间。

进入页面的方法：系统管理>>系统配置>>系统时间

时间信息

当前系统时间： 2006-01-01 10:43:28 星期日

当前时间来源： 手动配置时间

时间配置

手动配置时间

日期： 2006 01 01

时间： 10 43 28

获取GMT时间

时区： (GMT+08:00)北京，重庆，乌鲁木齐，香港特别行政区，台北

首选NTP服务器： 133.100.9.2

备选NTP服务器： 139.78.100.163

获取管理PC时间

提交 刷新

夏令时配置

夏令时状态: 禁用

开始时间： 04 01 00:00

结束时间： 10 01 00:00

提交 帮助

图 4-5 系统时间

条目介绍：

➢ 时间信息

当前系统时间：	显示交换机当前的日期、时间。
当前时间来源：	显示交换机当前系统时间的来源。

➢ 时间配置

手动配置时间：	勾选后，手动配置日期、时间。
获取 GMT 时间：	勾选后，配置时区和 NTP 服务器的 IP 地址，交换机将向 NTP 服务器不断发送请求包以获取 GMT 时间。此时交换机必须连接至 NTP 服务器。 ● 时区：选择您所在的时区。 ● 首选/备选 NTP 服务器：填写 NTP 服务器的 IP 地址。
获取管理 PC 时间：	勾选后，将管理主机的时间配置为交换机的系统时间。

➢ 夏令时配置

夏令时状态：	选择是否启用夏令时功能。
开始时间：	设置夏令时启动的日期和时间。
结束时间：	设置夏令时结束的日期和时间。


注意：

● 如果向指定的时间服务器请求时间不成功，交换机会选择向上一次成功获取时间的服务器地址和网络上默认的公用时间服务器地址来获取时间。

4.1.4 管理IP

网络中的设备都有自己的 IP 地址，您可以使用交换机的 IP 地址登录交换机的 Web 页面。本交换机提供“静态 IP”、“DHCP”和“BOOTP”三种 IP 获取方式，但交换机的 IP 地址是唯一的，所以使用新的配置方式获取的 IP 地址会覆盖原有的 IP 地址。

- “静态 IP”获取方式。

需要手动配置交换机的 IP 地址、子网掩码和默认网关，使用时应根据自己网络的实际情况对这些参数进行配置。管理主机的 IP 地址必须与此处所配置的 IP 地址处于同一网段内，才能访问交换机的 Web 页面。

- “DHCP”获取方式。

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是在 BOOTP 协议基础上进行了优化和扩展而产生的一种网络配置协议，可以实现网络资源的动态配置。交换机作为 DHCP 客户端，可以从网络中的 DHCP 服务器上动态获得网络参数，既方便配置，又便于管理。

- “BOOTP”获取方式。

BOOTP（Bootstrap Protocol，自举协议）。交换机作为 BOOTP 客户端，可以从 BOOTP 服务器获得网络参数。但是，在自动获取之前，网管需要在 BOOTP 服务器上为每个客户端配置 BOOTP 参数，所以 BOOTP 一般运行在相对稳定的网络环境中，当网络规模较大、变化频繁时，建议选择 DHCP 获取方式。

本页面用来配置交换机的管理 IP 地址。

进入页面的方法：系统管理>>系统配置>>管理 IP

IP配置

MAC地址： 00-00-54-28-00-04

获取方式： ◉静态IP ○DHCP ○BOOTP

管理VLAN： 1 （VLAN ID 1-4094）

IP地址： 192.168.0.1

子网掩码： 255.255.255.0

默认网关：

提交 帮助

注意：

IP地址的变更可能导致当前网络连接的中断，请保持IP地址与内网IP地址在同一网段。

图 4-6 管理 IP

条目介绍：

➢ **IP 配置**

MAC 地址： 显示交换机的物理地址。

获取方式： 选择交换机网络参数的获取方式。

- 静态 IP：手动填写交换机的 IP 地址、子网掩码和默认网关。
- DHCP：从网络中的 DHCP 服务器获取交换机的网络参数。
- BOOTP：从网络中的 BOOTP 服务器获取交换机的网络参数。

管理 VLAN：	配置交换机的管理 VLAN，只有连接到管理 VLAN 成员端口的计算机才可以通过 Web、telnet、SSL 或 SSH 等方式来管理交换机。 当你通过 Web 页面等方式来配置交换机的管理 VLAN 后，你可能无法再对交换机进行配置管理，请将管理计算机连接的交换机端口切换到管理 VLAN 的成员端口以便获得管理交换机的权限。
IP 地址：	填写交换机的管理 IP 地址。该 IP 地址出厂默认值为 192.168.0.1，您可以根据需要改变它。
子网掩码：	填写本交换机的子网掩码。
默认网关：	填写本交换机的默认网关。

注意：

- IP 地址的变更可能导致当前网络连接的中断，请保持 IP 地址与内网 IP 地址在同一网段。
- 交换机只有一个 IP 地址。新配置的 IP 地址将覆盖原有的 IP 地址。
- 当交换机通过 DHCP 服务器请求 IP 参数时，交换机会一直向网络发出申请，直到成功，你可以在给交换机分配 IP 参数的 DHCP 服务器上了解到交换机的配置信息。
- 交换机出厂时，默认的 IP 地址是：192.168.0.1。

4.2 用户管理

用户管理用来限制登录交换机 Web 页面的用户的访问权限和身份，以保护交换机的有效配置。

本功能包括**用户列表**和**用户配置**两个配置页面。

4.2.1 用户列表

可以在本页查看到当前交换机存在的全部用户。

进入页面的方法：系统管理>>用户管理>>用户列表



用户列表

序号	用户名	类型	状态
1	admin	管理员	启用

刷新

图 4-7 用户列表

4.2.2 用户配置

本页用来配置登录交换机 Web 页面的用户的身份类型。本交换机提供两种类型的用户：受限用户和管理员。受限用户，仅可以查看部分功能的配置数据，不能对交换机进行任何配置；管理员，可以配置交换机的全部功能。本说明书内如无特殊说明，均以“管理员”身份登录时的 Web 页面为准。

进入页面的方法：系统管理>>用户管理>>用户配置

用户信息

用户名：

用户类型： 受限用户

用户状态： 启用 禁用

密码：

确认密码：

添加

清除

用户列表

选择	序号	用户名	类型	状态	操作
☐	1	admin	管理员	启用	编辑

删除 帮助

注意：

用户名和密码只允许1-16个字符，且只能包含数字、英文字母和下划线。

图 4-8 用户配置

条目介绍：

➢ 用户信息

用户名： 填写登录 Web 页面的用户名。

用户类型： 选择该用户名的用户类型。

- 管理员：可以编辑、修改和查看交换机各个功能的配置。
- 受限用户：仅可以查看交换机各个功能的配置情况。

用户状态： 选择是否启用该用户。

密码： 填写该用户名的登录密码。

确认密码： 再次输入该用户名的登录密码，两次输入的密码需保持一致。

➢ 用户列表

选择： 勾选条目进行删除，可多选。但是不可以对当前登录用户自身进行删除。

序号、用户名、类型、状态： 显示当前用户的序号、用户名、用户类型和用户状态。

操作： 点击对应条目的<编辑>按键，可以修改该条目的用户信息。修改完毕后点击<修改>按键，修改内容生效。但是不允许修改当前登录用户自身的用户类型和状态。

4.3 系统工具

系统工具功能集中对交换机的配置文件进行管理，包括**配置导入**、**配置导出**、**软件升级**、**系统重启**和**系统复位**五个配置页面。

4.3.1 配置导入

配置导入功能是将以前备份的配置文件导入至交换机中，使交换机恢复到当时的配置状态。

进入页面的方法：系统管理>>系统工具>>配置导入

配置文件导入

从用户备份的配置文件中恢复配置信息。

选择一个以前备份的配置文件，然后点击"导入配置文件"按钮，可以恢复到当时的配置状态。

配置文件： 浏览…

导入配置文件 帮助

注意：

1、恢复配置可能需要较长时间，此期间请耐心等待，不要操作交换机。

图 4-9 配置导入

条目介绍：

➢ 配置文件导入

导入配置文件：	将备份文件中保存的配置信息恢复到当前状态，交换机自动重启后配置生效。

注意：

- 恢复配置可能需要较长时间，此期间请耐心等待，不要操作交换机。
- 导入配置文件的过程不能关闭交换机电源，否则将导致交换机损坏而无法使用。
- 导入配置文件后，交换机中原有的配置信息将会丢失。如果您导入的配置文件有误，可能会导致交换机无法被管理。

4.3.2 配置导出

配置导出功能是将交换机当前的配置信息打包成文件保存到 PC 中，方便您日后通过该文件恢复配置。

进入页面的方法：系统管理>>系统工具>>配置导出

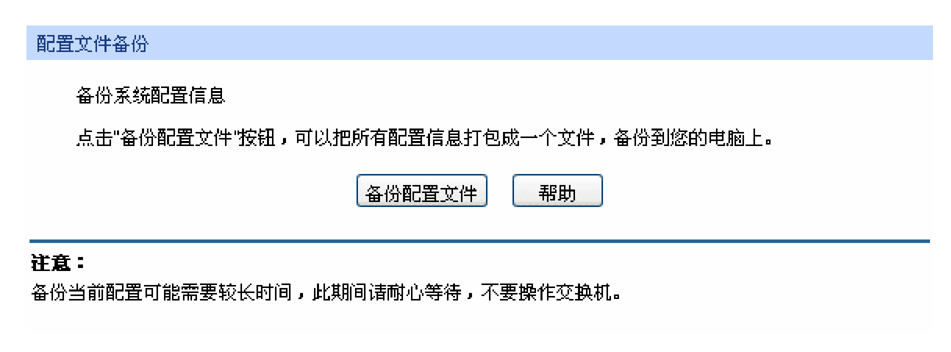


图 4-10 配置导出

条目介绍：

➢ 配置文件备份

备份配置文件： 以文件形式保存您的设置。建议升级前进行备份。

注意:

- 备份当前配置可能需要较长时间，此期间请耐心等待，不要操作交换机。

4.3.3 软件升级

本交换机可以通过 Web 方式升级系统文件，系统升级后将获得更完善的功能，请在 http://www.tp-link.com.cn 网站上下载最新版本的系统文件。

进入页面的方法：**系统管理>>系统工具>>软件升级**



图 4-11 软件升级

注意:

- 升级过程中不能被中断。
- 升级时请选择与当前硬件版本一致的软件。
- 升级过程需持续一段时间，在此期间不能关闭设备电源，否则将导致设备损坏而无法使用。
- 建议升级前备份您的配置信息。

4.3.4 系统重启

在此处可以重新启动交换机，交换机重启后自动返回到登录页面。重启前请先保存当前配置，否则重启后，未保存的配置信息将丢失。

进入页面的方法：**系统管理>>系统工具>>系统重启**

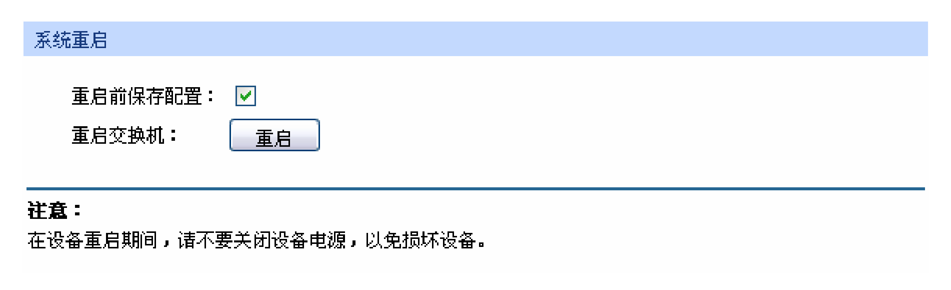


图 4-12 系统重启

注意:

- 在设备重启期间，请不要关闭设备电源，以免损坏设备。

4.3.5 软件复位

通过软件复位，可以将交换机恢复为出厂设置状态，所有配置数据将被清除。

进入页面的方法：系统管理>>系统工具>>软件复位

软件复位

软件复位： 复位

注意：
软件复位后，交换机配置将恢复成出厂默认状态，用户配置数据将丢失。

图 4-13 软件复位


注意:

- 软件复位后，交换机配置将恢复成出厂默认状态，您配置的数据将丢失。

4.4 安全管理

安全管理功能是针对不同的远程登录方式，采取相应的安全措施，以增强用户管理交换机的安全性。包括**安全配置**、**SSL 配置**、**SSH 配置**三个配置页面。

4.4.1 安全配置

本页用来限制登录交换机Web页面的用户的身份及人数，从而增强了交换机配置管理的安全性。其中，管理员及受限用户的定义请参考4.2 用户管理。

进入页面的方法：系统管理>>安全管理>>安全配置

身份限制

限制类型： 禁用

IP地址： 掩码：

MAC地址：

端口号：

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
25	26	27	28				

超时配置

超时时间： 10 分钟（5-30）

管理人数限制

人数限制功能： 启用 禁用

管理员人数： 名（1-16）

受限用户人数： 名（0-15）

提交 帮助

图 4-14 安全配置

条目介绍：

➢ 身份限制

限制类型： 选择限制用户身份的类型。

- 基于 IP：用来限制访问交换机 Web 页面的用户的 IP 网段。
- 基于 MAC：用来限制访问交换机 Web 页面的用户的主机 MAC 地址。
- 基于端口：用来限制访问交换机 Web 页面的交换机端口号。

IP 地址、掩码： 选择“基于 IP”时才能进行配置。只允许指定 IP 网段的用户才可以通过 Web 页面访问交换机。

MAC 地址： 选择“基于 MAC”时才能进行配置。只允许指定 MAC 地址的用户才可以通过 Web 页面访问交换机。

端口号： 选择“基于端口”时才能进行配置。只允许指定端口上的用户才可以通过 Web 页面访问交换机。

➢ 超时配置

超时时间： 如果在超时时间之内没有对交换机管理页面进行操作，系统会自动退出管理页面，若要再次进行管理请重新登录。默认为 10 分钟。

➢ 管理人数限制

人数限制功能： 选择是否启用人数限制功能。

管理员人数： 填写可同时登录交换机 Web 页面的管理员总数。

受限用户人数： 填写可同时登录交换机 Web 页面的受限用户总数。

4.4.2 SSL配置

SSL（Secure Sockets Layer，安全套接层）是一个安全协议，它为基于 TCP 的应用层协议提供安全连接，如为普通的 HTTP 连接提供更安全的 HTTPS 连接。SSL 协议广泛地用于 Web 浏览器与服务器之间的身份认证和加密数据传输，多使用在电子商务、网上银行等领域，为网络上数据通讯提供安全性保证。

SSL 协议提供的服务主要有：

1. 对用户和服务器进行基于证书的身份认证，确保数据发送到正确的用户和服务器；
2. 对传输数据进行加密，以防止数据中途被窃取；
3. 维护数据的完整性，确保数据在传输过程中不被改变。

SSL 采用非对称加密技术，使用“密钥对”进行数据的加密/解密，“密钥对”由一个公钥（包含在证书中）和一个私钥构成。初始时交换机里已有默认的证书（自签名）和对应私钥，也可以通过证书/密钥导入功能替换默认的密钥对，但 SSL 证书/密钥必须配对导入，否则 HTTPS 不能正常连接。

本功能生效后，即可通过https://192.168.0.1登录交换机的Web页面。初次使用交换机默认的证书通过HTTPS登陆交换机时，浏览器可能会提示“该证书是自签名的而不被信任”或“证书错误”，此时请将此证书添加为信任证书，或者继续浏览此网站即可。

进入页面的方法：系统管理>>安全管理>>SSL 配置

全局配置

SSL功能： 启用 禁用 提交 帮助

证书导入

SSL证书： 浏览… 导入证书

密钥导入

SSL密钥： 浏览… 导入密钥

注意：

1、SSL证书/密钥导入后，需要重启交换机才能生效。

2、SSL证书/密钥必须配对导入，否则HTTPS不能正常连接。

图 4-15 SSL 证书管理

条目介绍：

➢ **SSL 证书管理**

SSL 功能： 选择是否启用交换机的 SSL 功能。

➢ 证书导入

SSL 证书： 选择要导入的 SSL 证书。证书必须为 BASE64 编码格式。

➢ 密钥导入

SSL 密钥： 选择要导入的 SSL 密钥。密钥必须为 BASE64 编码格式。

注意：

- SSL 证书/密钥必须配对导入，否则 HTTPS 不能正常连接。
- SSL 证书/密钥导入后，需要重启交换机才能生效。
- 要使用 HTTPS 建立安全连接，必须在浏览器的地址栏指定“https://提示符”。
- HTTPS 连接涉及身份认证、加密、解密等过程，故响应速度可能会比普通的 HTTP 连接稍慢。

4.4.3 SSH配置

SSH（Secure Shell，安全外壳）是由 IETF（Internet Engineering Task Force，因特网工程任务组）所制定，建立在应用层和传输层基础上的安全协议。SSH 加密连接所提供的功能类似于一个 telnet 连接，但是传统的 telnet 远程管理方式在本质上是不安全的，因为它在网络上是使用明文传送口令和数据的，别有用心的人可以很容易的截获这些口令和数据。当通过一个不能保证安全的网络环境远程登录到设备时，SSH 功能可以提供强大的加密和认证安全保障，它可以对所有传输的数据进行加密，可以有效防止远程管理过程中的信息泄露问题。

SSH 是由服务器端和客户端组成的，并且有 V1 和 V2 两个不兼容的版本。在通讯过程中，SSH 服务器与客户端会自动互相协商 SSH 版本号和加密算法，协商一致后，由客户端向服务器端发起请求登录的认证请求，认证通过后双方即可进行信息的交互。本交换机支持 SSH 服务器功能，可以使用 SSH 客户端软件通过 SSH 连接方式登录交换机。

SSH 密钥导入是将 SSH 的公钥文件导入至交换机中。如果密钥导入成功，交换机会优先选用密钥认证的方式接受 SSH 登入。

进入页面的方法：系统管理>>安全管理>>SSH 配置

全局配置

SSH功能： 启用 禁用

Protocol V1： 启用 禁用

Protocol V2： 启用 禁用

静默时长： 500 秒（1-999）

最大连接数： 5 （1-5）

提交 帮助

密钥导入

选择你要导入交换机的密钥。

密钥类型： SSH-2 RSA/DSA 导入密钥

密钥文件： 浏览…

注意：

1、导入密钥可能需要较长时间，此期间请耐心等待，不要操作交换机。

图 4-16 SSH 配置

条目介绍：

➢ 全局配置

SSH 功能： 选择是否启用 SSH 功能。

Protocol V1： 选择是否启用对 SSH V1 的支持。

Protocol V2： 选择是否启用对 SSH V2 的支持。

静默时长： 填写静默时长。该时间内客户端无任何操作时，连接会自动断开。默认为 500 秒。

最大连接数： 填写 SSH 同时可允许的最大连接数，连接数若满，将无法再建立新的连接。默认为 5。

➢ 密钥导入

密钥类型： 选择所要导入的密钥类型。本机支持 SSH-1 RSA,SSH-2 RSA 和 SSH-2 DSA 三种类型的密钥。

密钥文件： 选择要导入的密钥文件。

导入密钥： 点击此按键，将所选的 SSH 密钥导入交换机。

注意：

- 请确保导入的文件是密钥长度为 256 至 3072 比特的 SSH 公钥。
- 导入密钥文件后，交换机中此用户原有的同类型密钥将会被覆盖。如果您导入的密钥文件有误，SSH 会转用密码认证的方式登陆。

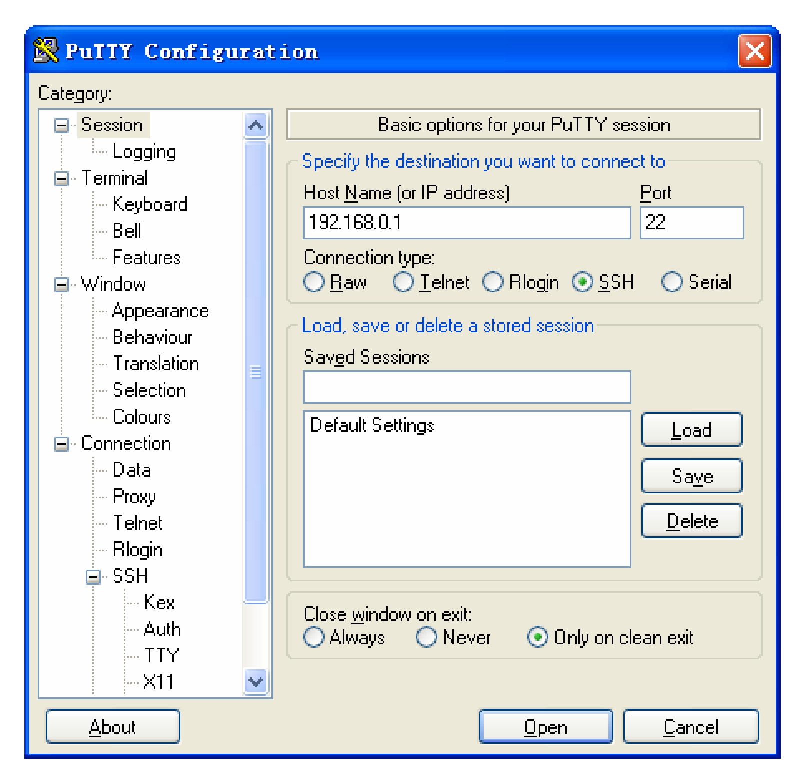
组网应用 1：

➢ 组网需求

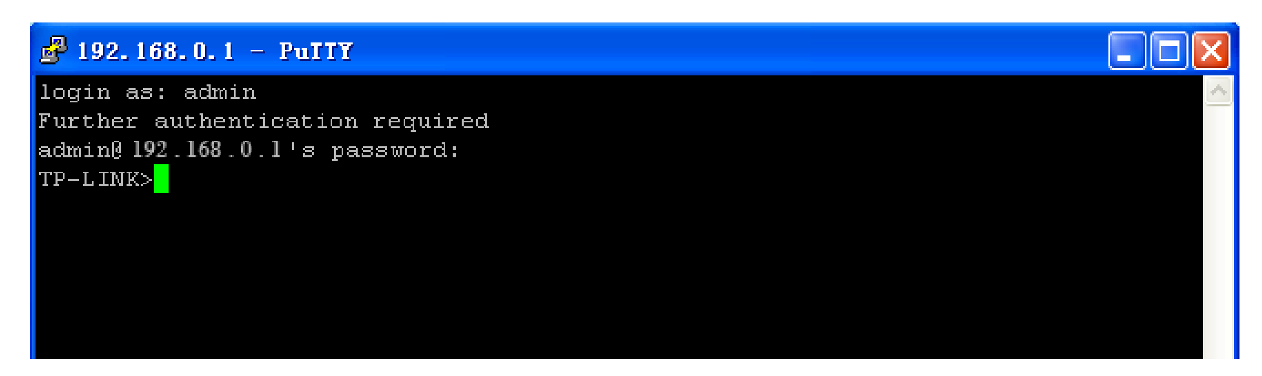
1. 使用 SSH 功能的“密码认证”的方式登录交换机，交换机已启用 SSH 功能。
2. 推荐使用第三方客户端软件 PuTTY。

➢ 配置步骤

1. 打开软件，登录 PuTTY 的主界面。在“Host Name”处填写交换机的 IP 地址；“Port”保持默认的 **22**；“Connection type”处选择 **SSH** 的接入方式。如下图所示。



2. 点击<Open>按键，即可登录到交换机。操作方法与 telnet 相同，输入登录用户名和登录密码，即可继续进行配置操作。如下图所示。



组网应用 2：

➢ 组网需求

1. 使用 SSH 功能的“密钥认证”的方式登录交换机，交换机已启用 SSH 功能。
2. 推荐使用第三方客户端软件 PuTTY。

➢ 配置步骤

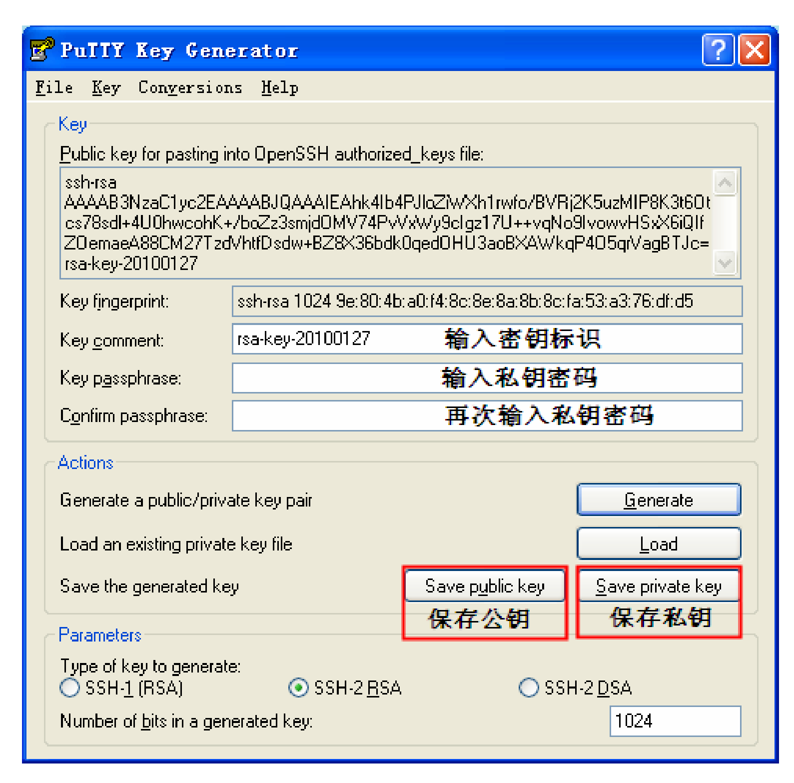
1. 选择密钥类型和密钥长度，并生成 SSH 密钥。如下图所示。



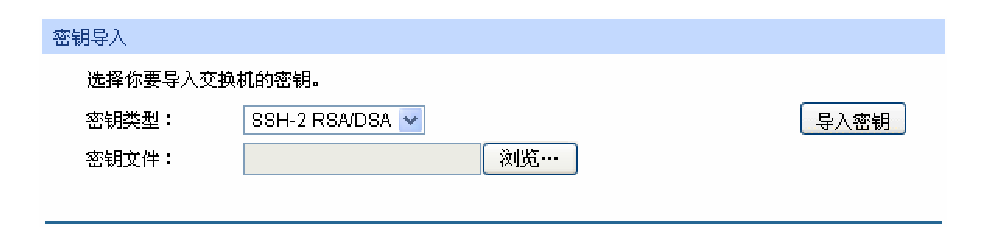
注意：

- 密钥长度的范围为 256 至 3072 比特。
- 生成密钥的过程中，在软件的空白处快速的随意晃动鼠标，产生随机数据，可以加快密钥生成的速度。

2. 密钥生成后，将公钥和私钥文件保存在主机上。如下图所示。



3. 在交换机配置页面上，将保存至主机上的公钥文件导入交换机中。



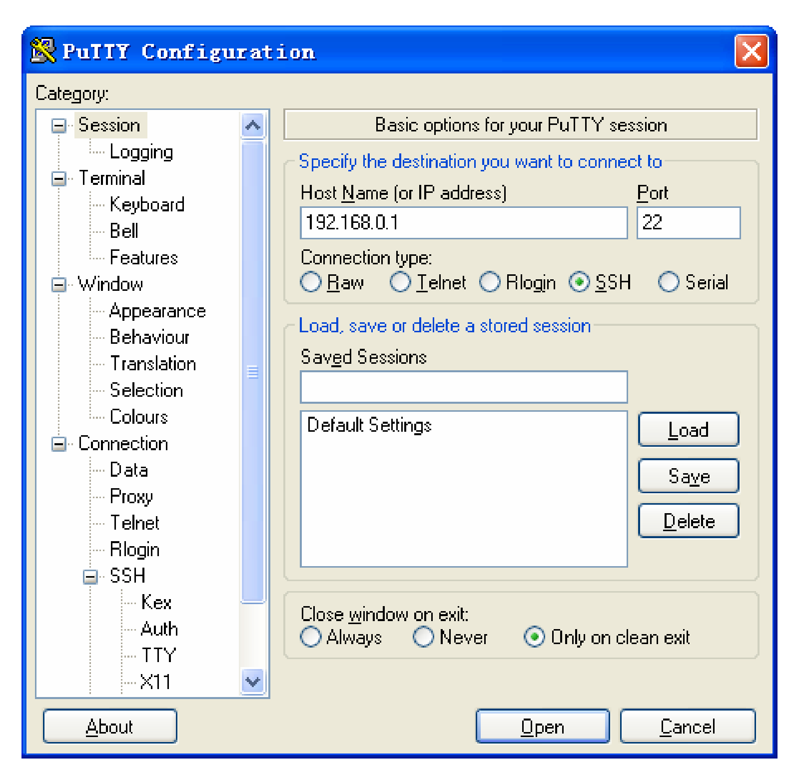
注 意：

- 密钥类型要与密钥文件的类型保持一致。
- 载入 SSH 密钥的过程不能被中断。

4. 将私钥文件导入至 SSH 客户端软件中。如下图所示。



5. 经过上面步骤后，公钥和私钥文件都已导入，接着即可进入版本、密钥与算法协商配置操作。打开 PuTTY 的主界面，输入 IP 地址并选择连接类型为 SSH 后，点击<open>按钮与服务器建立连接并进行协商。



6. 协商成功后，输入用户名进行登录，如果你不需要输入密码即可登陆成功，表明密钥认证已经成功。如下图所示。



回目录

第5章 二层交换

二层交换模块主要用于配置交换机的基本功能，包括**端口管理**、**汇聚管理**、**流量统计**以及**地址表管理**四个部分。

5.1 端口管理

端口管理用于配置交换机端口的基本属性，包括**端口配置**、**端口监控**、**端口安全**和**端口隔离**四个功能配置页面。

5.1.1 端口配置

端口配置用来配置交换机端口的各项基本参数。端口状态选择“禁用”时，交换机将丢弃来自这个端口的数据包。当交换机端口长时间不使用时，可以将该端口设为禁用，可有效减小交换机的功耗，待使用时再将该端口设为启用。

端口基本参数将会直接影响端口的工作方式，请结合实际情况进行配置。

进入页面的方法：二层交换>>端口管理>>端口配置



选择	端口	描述	状态	速率双工	流控	LAG
☐	1		启用	Auto	禁用	---
☐	2		启用	Auto	禁用	---
☐	3		启用	Auto	禁用	---
☐	4		启用	Auto	禁用	---
☐	5		启用	Auto	禁用	---
☐	6		启用	Auto	禁用	---
☐	7		启用	Auto	禁用	---
☐	8		启用	Auto	禁用	---
☐	9		启用	Auto	禁用	---
☐	10		启用	Auto	禁用	---
☐	11		启用	Auto	禁用	---
☐	12		启用	Auto	禁用	---
☐	13		启用	Auto	禁用	---
☐	14		启用	Auto	禁用	---
☐	15		启用	Auto	禁用	---

图 5-1 端口配置

条目介绍：

➢ 端口配置

端口选择：	点击<选择>按键，可根据所输端口号，快速选择相应端口。
选择：	勾选端口配置端口参数，可多选。
端口：	显示交换机的端口号。
描述：	填写端口的描述信息，便于您区分各个端口的用途。

状态： 选择端口状态。只有状态为启用时，端口才能正常转发数据包。

速率双工： 选择端口的传输速率及传输模式。与交换机相连的设备必须与交换机的传输速率及双工状态保持一致。当选择“Auto”选项时，该端口的速率双工由自动协商决定。默认为 Auto。

流控： 选择端口的流控状态。启用流控能够同步接收端和发送端的速度，防止因速率不一致导致的网络丢包。

LAG： 显示端口当前所属的汇聚组。

注意：

- 端口状态配置为禁用则不能通过该端口管理交换机，请将要进行管理的端口配置为启用状态。
- 从属于同一个汇聚组的所有成员端口的相应参数配置应该保持一致。

5.1.2 端口监控

端口监控是一种数据包获取技术，通过配置交换机，可以实现将一个/几个端口（被监控端口）的数据包复制到一个特定的端口（监控端口），在监控端口接有一台安装了数据包分析软件的主机，对收集到的数据包进行分析，从而达到了网络监控和排除网络故障的目的。

进入页面的方法：二层交换**>>**端口管理**>>**端口监控



图 5-2 端口监控

条目介绍：

➢ 监控端口配置

选择监控端口： 选择物理端口作为监控端口，您可在此端口连接数据检测设备，当选择“禁用”选项时将禁止端口监控。

➢ 被监控端口配置

端口选择：	点击<选择>按键，可根据所输端口号，快速选择相应端口。
选择：	勾选端口配置为被监控端口，可多选。
端口：	显示交换机的端口号。
入口监控：	对被监控端口收到的数据进行监控，复制到监控端口。
出口监控：	对被监控端口发出的数据进行监控，复制到监控端口。
LAG：	显示端口当前所属的汇聚组。汇聚组成员端口不能选为监控端口和被监控端口。

注意：

- 汇聚组的成员端口既不能作为监控端口，也不能作为被监控端口。
- 一个端口不可以既作为监控端口又作为被监控端口。
- 端口监控功能可以跨越 VLAN 进行监控。

5.1.3 端口安全

交换机地址表维护着端口和接入端的 MAC 地址的对应关系，并以此建立交换路径，地址表的大小是固定的。地址表攻击是指利用工具产生欺骗 MAC，快速填满地址表，交换机地址表被填满后，交换机将以广播方式处理通过交换机的报文，这时攻击者可以利用各种嗅探，攻击获取网络信息。地址表满了后，数据流以洪泛的方式发送到所有端口，会造成交换机负载过大，网络缓慢和丢包甚至瘫痪。

端口安全通过限制端口的最大学习 MAC 数目，来防范 MAC 地址攻击并控制端口的网络流量。如果端口启用端口安全功能，将动态学习接入的 MAC 地址，当学习地址数达到最大值时停止学习。此后，MAC 地址未被学习的网络设备将不能再通过该端口接入网络，以保证安全性。

进入页面的方法：二层交换>>端口管理>>端口安全

端口安全

选择	端口	最大学习地址数	已学习地址数	学习模式	状态
☐				动态	禁用
☐	1	64	0	动态	禁用
☐	2	64	0	动态	禁用
☐	3	64	0	动态	禁用
☐	4	64	0	动态	禁用
☐	5	64	0	动态	禁用
☐	6	64	0	动态	禁用
☐	7	64	0	动态	禁用
☐	8	64	0	动态	禁用
☐	9	64	0	动态	禁用
☐	10	64	0	动态	禁用
☐	11	64	0	动态	禁用
☐	12	64	0	动态	禁用

提交　帮助

注意：
最大学习地址数的范围为0-64。

图 5-3 端口安全

条目介绍：

➢ 端口安全

选择： 勾选端口配置端口安全，可多选。

端口： 显示交换机的端口号。

最大学习地址数： 填写对应端口最多可以学习的 MAC 地址数目。默认为 64。

已学习地址数： 显示对应端口已经学习的 MAC 地址数目。

学习模式： 选择 MAC 地址学习的模式。

- 动态：MAC 地址学习受老化时间的限制，老化时间过后，所学的 MAC 地址将被删除。
- 静态：MAC 地址学习不受老化时间的限制，只能手动进行删除。交换机重启后该条目清空。
- 永久：MAC 地址学习不受老化时间的限制，只能手动进行删除。交换机重启后该条目保持不变。

状态： 选择是否启用端口安全功能。


注意：

- 当端口为汇聚组成员，该端口的端口安全功能被禁用。只有将端口从汇聚组中去掉，才可以使用端口的端口安全功能。
- 若 802.1X 模块启用，此功能禁用。

5.1.4 端口隔离

通过端口隔离功能，可以为交换机的任意物理端口指定转发端口。设置了端口隔离功能后，每个物理端口只能向自己的转发端口转发数据包。

进入页面的方法：二层交换>>端口管理>>端口隔离

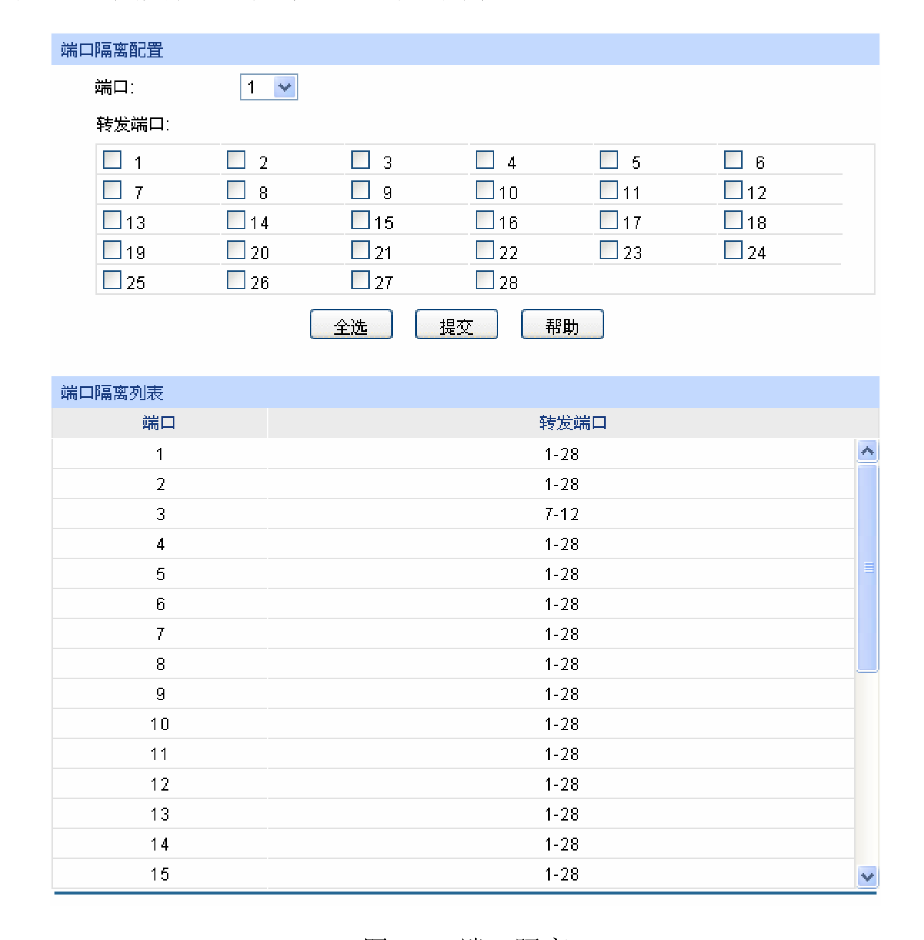


图 5-4 端口隔离

条目介绍：

➤ 端口隔离配置

端口：　　选择一个物理端口，以配置其转发端口。

转发端口：　　选择报文可以被转发到的端口。

➤ 端口隔离列表

端口：　　显示交换机的端口号。

转发端口：　　显示可转发的端口列表。

5.2 汇聚管理

LAG(Link Aggregation Group，端口汇聚组)是将交换机的多个物理端口汇聚在一起形成一个逻辑端口，同一汇聚组内的多条链路可视为一条逻辑链路。端口汇聚可以实现流量在汇聚组中各个成员端口之间进行分担，以增加带宽。同时，同一汇聚组的各个成员端口之间彼此动态备份，提高了连接可靠性。

属于同一个汇聚组中的成员端口必须有一致的配置，这些配置主要包括 STP、QoS、GVRP、VLAN、

端口属性、MAC 地址学习等。具体说明如下：

- 开启 **GVRP**、**802.1Q VLAN**、**语音 VLAN**、**生成树**、**QoS 配置**、**DHCP 侦听**及**端口配置**（速率双工、流控）功能的端口，若属于汇聚组成员，则它们的配置需保持一致。
- 开启**端口安全**、**端口监控**、**MAC 地址过滤**、**静态 MAC 地址绑定**、**802.1X 认证**、**IP 源防护**功能的端口，不能加入汇聚组。
- 开启 **ARP 防护**、**DoS 防护**功能的端口，建议不要将其加入汇聚组。

如果您需要配置汇聚组，建议您在本功能处优先配置汇聚组后，再去其它功能处配置汇聚组的其它功能。

说明：

- LAG 带宽的计算：当使用四个全双工 1000Mbps 端口构成 LAG 时，由于每一个端口上行和下行各是 1000Mbps，所以每一个端口的带宽为 2000Mbps。它们使用 LAG 技术汇聚在一起形成的总带宽为 8000Mbps。
- LAG 的流量会根据选路算法均衡分配到各个成员端口中。当 LAG 中的一个或几个端口连接断开的时候，这些端口的流量会转移到 LAG 中其它链接正常的端口中，具备链路冗余备份功能。

按照汇聚方式的不同，端口汇聚可以分为两类：手动配置和 LACP 配置。本功能包括**汇聚列表**、**手动配置**和 **LACP 配置**三个配置页面。

5.2.1 汇聚列表

在本页，您可以查看到交换机当前的全部汇聚组。

进入页面的方法：二层交换>>汇聚管理>>汇聚列表

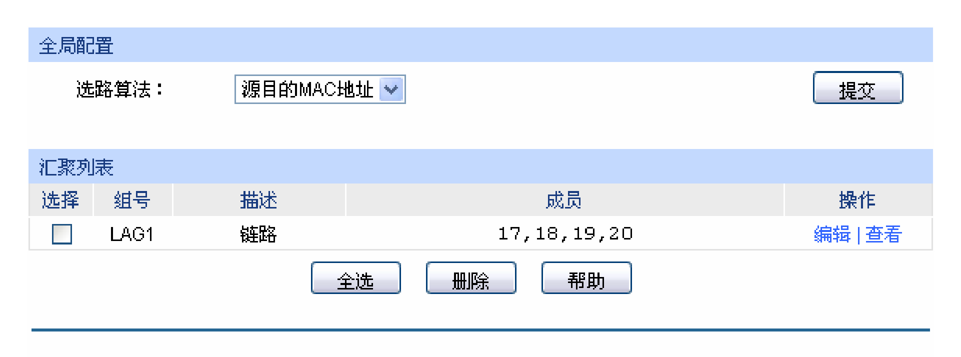


图 5-5 汇聚列表

条目介绍：

- 全局配置

选路算法： 根据选路算法规则，选择转发数据的端口。

- 源目的 MAC 地址：仅使用数据包中的源目的 MAC 地址信息。
- 源目的 IP 地址：仅使用数据包中的源目的 IP 地址信息。

- 汇聚列表

选择： 勾选汇聚组进行删除，可多选。

组号： 显示汇聚组的序号。

描述： 显示汇聚组的描述信息。

成员： 显示属于汇聚组的物理端口。

操作： 对单个汇聚组进行相应配置。

- 编辑：修改汇聚组的描述和成员端口。
- 查看：查看汇聚组的端口状态信息。

点击<查看>按键，您可以看到所选汇聚组的详细信息。



图 5-6 汇聚组状态

5.2.2 手动配置

您可以在本页对汇聚组进行手动配置，手动配置的汇聚端口的 LACP 状态为禁用。

进入页面的方法：二层交换>>汇聚管理>>手动配置

汇聚组配置

选择组号： LAG1

该组描述： 链路 （最多16个英文字符或8个汉字）

成员端口

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6
☐ 7	☐ 8	☐ 9	☐ 10	☐ 11	☐ 12
☐ 13	☐ 14	☐ 15	☐ 16	☑ 17 (LAG1)	☑ 18 (LAG1)
☑ 19 (LAG1)	☑ 20 (LAG1)	☐ 21	☐ 22	☐ 23	☐ 24
☐ 25	☐ 26	☐ 27	☐ 28		

提交 清空 帮助

注意：

1、LAG*表示该端口当前所属的汇聚组(Link Aggregation Group)。

2、不推荐一个汇聚组内同时有100M端口和1000M端口。

图 5-7 手动配置

条目介绍：

➢ 全局配置

选择组号：	选择汇聚组的序号，组号格式为 LAG*。
该组描述：	填写汇聚组的描述信息，便于您区分各个汇聚组的用途。

➢ 成员端口

成员端口：	勾选属于汇聚组的物理端口，清空表示删除该汇聚组。

说明：

- 要删除一个已配置的 LAG，将该 LAG 的成员清空并提交即可。
- 一个端口仅可以处于一个汇聚组中。即若端口已成为其它 LAG 的成员端口，或者已汇聚成为 LACP 中的成员时，该端口处于灰化状态，不能勾选。

5.2.3 LACP配置

LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是基于 IEEE802.3ad 标准用来实现链路动态汇聚与解汇聚的协议。汇聚的双方通过协议交互汇聚信息，将匹配的链路汇聚在一起收发数据，汇聚组内端口的添加和删除是协议自动完成的，具有很高的灵活性并提供了负载均衡的能力。

启用端口的 LACP 功能后，该端口向对端通告本端的汇聚标识（由系统优先级、系统 MAC、和管理 Key 组成），链路两端的汇聚标识完全一致才拥有汇聚在一起形成链路汇聚的条件。由于一台交换机最多只能生成 14 个链路汇聚组，因此当配置的汇聚组比较多的时候，系统优先级值小的会优先汇聚。同样，一个汇聚组内最多只能有 8 个成员端口，因此形成汇聚组的端口也有优先级的考虑，端口优先级值小的端口会被优先选择，当端口优先级相同时，优先选取端口号比较小的端口。

您可以在本页配置交换机的 LACP 功能。

进入页面的方法：二层交换>>汇聚管理>>LACP 配置

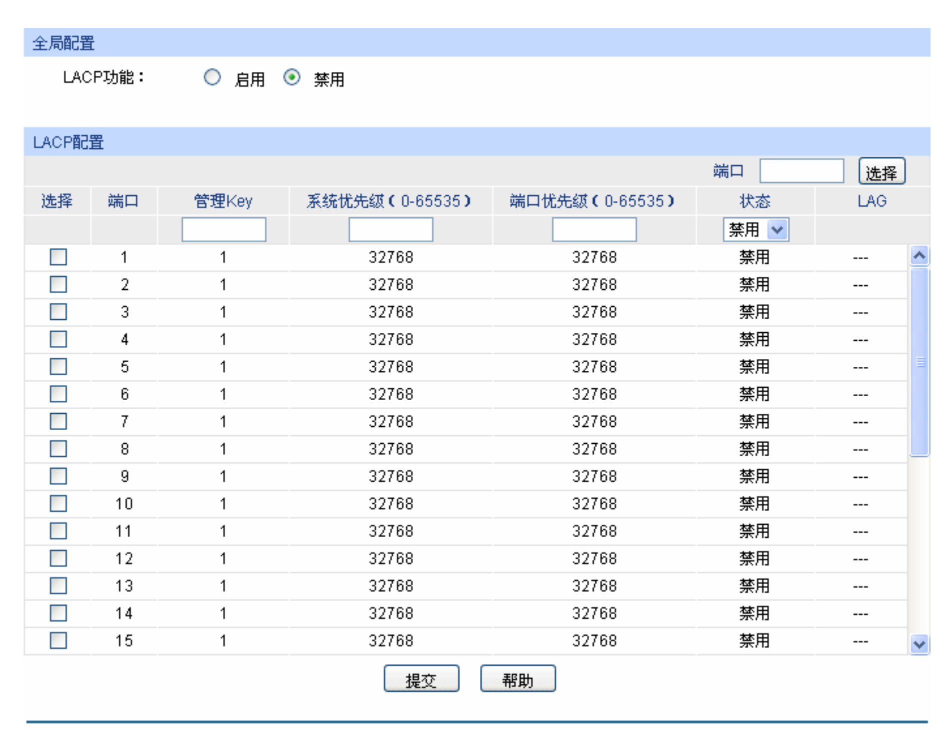


图 5-8 LACP 配置

条目介绍：

➢ 全局配置

LACP 功能： 选择是否启用交换机的 LACP 功能。

➢ LACP 配置

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

选择： 勾选端口配置端口 LACP 功能，可多选。

端口： 显示交换机的端口号。

管理 Key： 处于同一汇聚组的成员，需配置相同的管理 Key。

系统优先级： 与管理 Key 和系统的 MAC 地址共同形成链路本端的汇聚标识，汇聚标识完全一致的链路才拥有形成链路汇聚的条件。默认为 32768。

端口优先级： 决定了成为汇聚组成员的端口的优先级。端口优先级值小的端口会被选择为动态汇聚组成员。若端口优先级相同，则端口号小的会被选择为动态汇聚组成员。默认为 32768。

状态： 选择相应端口是否启用 LACP 功能。

LAG： 显示端口当前所属的汇聚组。

5.3 流量统计

流量统计用于统计流经各个端口的数据信息，本功能包括**流量概览**和**详细统计**两个配置页面。

5.3.1 流量概览

流量概览用来显示交换机各端口的流量信息，便于您监控网络流量和分析网络异常。

进入页面的方法：二层交换**>>**流量统计**>>**流量概览



图 5-9 流量概览

条目介绍：

➢ 自动刷新

自动刷新：	选择是否启用自动刷新功能。
刷新周期：	填写自动刷新的时间周期。默认为 30 秒。

➢ 流量概览

端口选择：	点击<选择>按键，可根据所输端口号，快速查找端口条目。
端口：	显示交换机的端口号。
接收数据包数：	统计交换机各端口接收的数据包数，不包括错误的数据包。
发送数据包数：	统计交换机各端口发送的数据包数。
接收字节数：	统计交换机各端口接收的字节数，包括错误的数据包的字节数。
发送字节数：	统计交换机各端口发送的字节数。
信息查询：	点击查询相应端口的详细统计信息。

5.3.2 详细统计

详细统计用来统计各端口传输数据包的详细信息，便于您定位网络问题。

进入页面的方法：二层交换>>流量统计>>详细统计



图 5-10 详细统计

条目介绍：

➢ 自动刷新

自动刷新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。

➢ 详细统计

端口： 输入您所要查看流量信息的交换机端口号。

接收信息统计： 统计该端口接收数据包的详细信息。

发送信息统计： 统计该端口发送数据包的详细信息。

广播包： 端口接收/发送的含有效广播地址的数据包数目（不含错误帧）。

多播包： 端口接收/发送的含有效多播地址的数据包数目（不含错误帧）。

单播包： 端口接收/发送的含有效单播地址的数据包数目（不含错误帧）。

Alignment 错误包： 端口接收的长度为 64-1518 字节的校验和错误的数据帧数目。

小于 64 字节包： 端口接收的长度小于 64 字节的数据帧数目（不含错误帧）。

64 字节包： 端口接收的长度为 64 字节的数据帧数目（包含错误帧）。

65-127 字节包： 端口接收的长度为 65-127 字节的数据帧数目（包含错误帧）。

128-255 字节包： 端口接收的长度为 128-255 字节的数据帧数目（包含错误帧）。

256-511 字节包： 端口接收的长度为 256-511 字节的数据帧数目（包含错误帧）。

512-1023 字节包： 端口接收的长度为 512-1023 字节的数据帧数目（包含错误帧）。

1024-2044 字节包： 端口接收的长度大于 1024 字节小于 2044 字节的数据帧数目（包含错误帧）。

冲突包： 端口工作在半双工模式下发送数据包时产生的冲突包数目。

5.4 地址表管理

交换机的主要功能是对报文进行转发，也就是根据报文的目的 MAC 地址将报文输出到相应的端口。地址表包含了端口间报文转发的地址信息，是交换机实现报文快速转发的基础。地址表中的表项可以通过自动学习和手动绑定两种方式进行更新和维护，多数地址表条目都是通过自动学习功能来创建和维护的，而对于某些相对固定的连接来说，手动绑定可以提高交换机的效率，通过 MAC 地址过滤功能可以使交换机对不期望转发的数据帧进行过滤，从而提升了网络安全性。

地址表的分类及特点如下表所示：

地址表类别	配置方式	有无老化时间	重启后是否被保留（配置保存后）	已绑定的 **MAC** 地址与端口的关系
静态地址表	手动配置	无	是	在同一 VLAN 中，已绑定的 MAC 地址不能被其它端口学习
动态地址表	自动学习	有	否	已绑定的 MAC 地址可以重新被其它端口学习
过滤地址表	手动配置	无	是	-

本功能包括**地址表显示**、**静态地址表**、**动态地址表**和**过滤地址表**四个配置页面。

5.4.1 地址表显示

在本页可以查看到交换机地址表的全部信息。

进入页面的方法：二层交换>>地址表管理>>地址表显示

显示配置

MAC地址： （格式为：00-00-00-00-00-01）

VLAN ID： （1-4094） 显示

端口： 端口 1 帮助

地址类型： 全部 静态 动态 过滤

地址表

MAC地址	VLAN ID	端口	地址类型	老化状态
00-19-66-35-E1-11	1	2	动态地址	正在老化
00-19-66-CA-87-E7	1	2	动态地址	正在老化
00-19-66-CA-87-CB	1	2	动态地址	正在老化
00-23-AE-08-E3-63	1	2	动态地址	正在老化
00-19-66-80-F8-A3	1	2	动态地址	正在老化
00-19-66-CA-64-FA	1	2	动态地址	正在老化
00-19-66-82-9A-4D	1	2	动态地址	正在老化
00-19-66-82-9A-4C	1	2	动态地址	正在老化
00-19-66-5E-EC-11	1	2	动态地址	正在老化
00-19-66-CB-44-E5	1	2	动态地址	正在老化
00-19-66-CB-44-D9	1	2	动态地址	正在老化
00-19-66-CB-44-D8	1	2	动态地址	正在老化

当前地址总数： 58

注意：

默认显示条目上限为100条，请点击显示按钮获取完整的地址表信息。

图 5-11 地址表显示

条目介绍：

➢ 显示配置

MAC 地址： 填写欲查找条目需包含的 MAC 地址信息。

VLAN ID： 填写欲查找条目需包含的 VLAN ID 信息。

端口： 选择欲查找条目需包含的交换机端口。

地址类型： 选择欲查找条目需包含的地址类型信息。

- 全部：显示全部地址表条目。
- 静态：显示静态地址表条目。
- 动态：显示动态地址表条目。
- 过滤：显示过滤地址表条目。

➢ 地址表

MAC 地址： 显示交换机学习到的 MAC 地址。

VLAN ID： 显示 MAC 地址条目对应的 VLAN ID。

端口： 显示 MAC 地址条目对应的交换机端口。

地址类型： 显示 MAC 地址的类型。

老化状态： 显示 MAC 地址的老化状态。

5.4.2 静态地址表

静态地址表记录了端口上配置的静态地址。静态地址是不会老化的 MAC 地址，它区别于一般的由端口学习得到的动态地址。静态地址只能手动添加和删除，不受最大老化时间的限制。这对于某些相对固定的连接来说，可减少地址学习步骤，从而提高交换机的转发效率。静态地址表也可以显示在**端口安全**功能中自动学习到的静态 MAC 地址。

进入页面的方法：二层交换>>地址表管理>>静态地址表

新建条目

MAC地址：（格式为：00-00-00-00-00-01）

VLAN ID：（1-4094） 添加

端口：端口 1

查找条目

查找选项：全部 查找

静态地址表

选择	MAC地址	VLAN ID	端口	地址类型	老化状态
☐			端口 1		

提交 删除 帮助

当前地址总数：0

注意：

默认显示的条目数上限值为100条，请点击查找按钮获取完整的地址表信息。

图 5-12 静态地址表

条目介绍：

➢ 新建条目

MAC 地址： 填写静态绑定的 MAC 地址。

VLAN ID： 填写 MAC 地址条目对应的 VLAN ID。

端口： 选择静态绑定的交换机端口号。

➢ 查找条目

查找选项： 选择静态地址表的显示规则，可以帮助您快速查找到所需的条目。

- MAC：填写欲查找条目需包含的 MAC 地址信息。
- VLAN ID：填写欲查找条目需包含的 VLAN ID 信息。
- 端口号：配置欲查找条目需包含的交换机端口号。

➢ 静态地址表

选择： 勾选条目进行删除或修改该条目对应的交换机端口号，可多选。

MAC 地址： 显示静态绑定的 MAC 地址。

VLAN ID： 显示 MAC 地址条目对应的 VLAN ID。

端口： 显示 MAC 地址条目对应的交换机端口。您可以在此修改与静态MAC地址绑定的端口，但是修改后的端口必须是VLAN的成员端口。

地址类型： 显示 MAC 地址的类型。

老化状态： 显示 MAC 地址的老化状态。

注意：

- 如果地址的端口指定错误，或使用过程中端口（或设备）被人为改变，必须重新设置该静态地址表项，否则交换机将无法正确转发数据。
- 静态地址一旦被设置，如果把有此地址的网络设备连接到交换机的其它端口，交换机将不能动态识别。因此必须保证静态地址表中的表项都是正确有效的。
- 凡是加入到静态地址表的地址，不能同时加入到过滤地址表，也不能被端口动态绑定。
- 若 802.1X 模块开启，此功能禁用。

5.4.3 动态地址表

动态地址是交换机通过自动学习获取的 MAC 地址，交换机通过自动学习和老化来不断更新其动态地址表。

交换机的地址表的容量是有限的，为了最大限度利用地址表的资源，交换机使用老化机制来更新地址表，即：系统在动态学习地址的同时，开启老化定时器，如果在老化时间内没有再次收到相同地址的报文，交换机就会把该 MAC 地址从表项删除。

在本页可以配置交换机的动态地址表功能。

进入页面的方法：二层交换>>地址表管理>>动态地址表

老化配置

自动老化： ◉ 启用 ○ 禁用

老化时间： 300 秒（10-630秒，默认为300秒） 提交

查找条目

查找选项： 全部 查找

动态地址表

选择	MAC地址	VLAN ID	端口	地址类型	老化状态
☐	00-19-66-80-54-36	1	9	动态地址	正在老化

全选 删除 绑定 帮助

当前地址总数： 1

注意：

默认显示的条目数上限值为100条，请点击查找按钮获取完整的地址表信息。

图 5-13 动态地址表

条目介绍：

➢ 老化设置

自动老化： 选择是否启用自动老化。

老化时间： 填写您需要的地址老化时间。默认为 300 秒。

➢ 查找条目

查找选项： 选择动态地址表的显示规则，可以帮助您快速查找到所需的条目。

- MAC：填写欲查找条目需包含的 MAC 地址信息。
- VLAN ID：填写欲查找条目需包含的 VLAN ID 信息。
- 端口号：选择欲查找条目需包含的交换机端口号。

➢ 动态地址表

选择： 勾选动态地址条目进行删除或将该条目绑定为静态地址，可多选。

MAC 地址： 显示动态绑定的 MAC 地址。

VLAN ID： 显示 MAC 地址条目对应的 VLAN ID。

端口： 显示 MAC 地址条目对应的交换机端口。

地址类型： 显示 MAC 地址的类型。

老化状态： 显示 MAC 地址的老化状态。

绑定： 将动态绑定的地址条目转化为静态绑定。

说明：

- 老化时间过长会导致交换机的地址表中保存过多过时的地址表项，从而耗尽地址表的资源，导致交换机无法根据网络的变化更新地址表。老化时间过短，又会造成地址表刷新过快，大量接收到的数据包的目的地址在地址表中找不到，致使交换机只能将这些数据包广播给所有端口，这将降低交换机的性能。建议您使用默认值。

5.4.4 过滤地址表

通过配置过滤地址，允许交换机对不期望转发的数据帧进行过滤，过滤地址不会被老化，只能手工进行添加和删除。在过滤地址表中添加受限的 MAC 地址后，交换机将自动过滤掉源/目的地址为这个地址的帧，以达到安全的目的。过滤地址表中的地址对所有的交换机端口都生效。

进入页面的方法：二层交换>>地址表管理>>过滤地址表

新建条目

MAC地址：　　（格式为：00-00-00-00-00-01）

VLAN ID：　　（1-4094）　　添加

查找条目

查找选项：　全部　　查找

过滤地址表

选择	MAC地址	VLAN ID	端口	地址类型	老化状态

全选　删除　帮助

当前地址总数：0

注意：

默认显示的条目数上限值为100条，请点击查找按钮获取完整的地址表信息。

图 5-14 过滤地址表

条目介绍：

➢ 新建条目

MAC 地址： 填写过滤的 MAC 地址。

VLAN ID： 填写 MAC 地址条目对应的 VLAN ID。

➢ 查找条目

查找选项： 选择过滤地址表的显示规则，可以帮助您快速查找到所需的条目。

- MAC：填写欲查找条目需包含的 MAC 地址信息。
- VLAN ID：填写欲查找条目需包含的 VLAN ID 信息。

➢ 静态地址表

选择： 勾选过滤地址条目进行删除，可多选。

MAC 地址： 显示过滤的 MAC 地址。

VLAN ID： 显示 MAC 地址条目对应的 VLAN ID。

端口号： 此处为"--"，表示无指定端口。

地址类型： 显示 MAC 地址的类型。

老化状态： 显示 MAC 地址的老化状态。

注意：

- 已加入到过滤地址表中的地址不能被加入到静态地址表中，也不能被端口动态绑定。
- 若 802.1X 模块开启，此功能禁用。

回目录

第6章 VLAN

以太网是一种基于CSMA/CD（Carrier Sense Multiple Access/Collision Detect，载波侦听多路访问/冲突检测）的共享通讯介质的数据网络通讯技术，当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降甚至使网络不可用等问题。通过交换机实现LAN互联虽然可以解决冲突（Collision）严重的问题，但仍然不能隔离广播报文。在这种情况下出现了VLAN（Virtual Local Area Network）技术，这种技术可以把一个LAN划分成多个逻辑的LAN——VLAN，每个VLAN是一个广播域，VLAN内的主机间通信就和在一个LAN内一样，而VLAN间则不能直接互通，这样，广播报文被限制在一个VLAN内。同一个VLAN内的主机通过传统的以太网通信方式进行报文的交互，而不同VLAN内的主机之间则需要通过路由器或三层交换机等网络层设备进行通信。如图6-1所示。

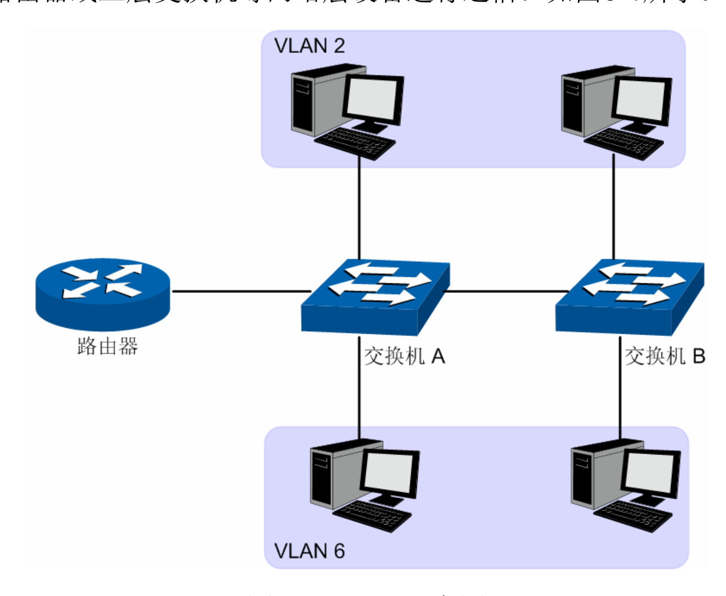


图6-1 VLAN 示意图

VLAN 的优点如下：

1) 提高网络性能。将广播包限制在 VLAN 内，从而有效控制网络的广播风暴，节省了网络带宽，从而提高网络处理能力。

2) 增强网络安全。不同 VLAN 的设备不能互相访问，不同 VLAN 的主机不能直接通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发。

3) 简化网络管理。同一个虚拟工作组的主机不会局限在某个物理范围内，简化了网络的管理，方便了不同区域的人建立工作组。

VLAN 的划分不受物理位置的限制，不在同一物理位置范围的主机可以属于同一个 VLAN；一个 VLAN 包含的用户可以连接在同一个交换机上，也可以跨越交换机。本交换机支持的 VLAN 划分方式包括 802.1Q VLAN、MAC VLAN 和协议 VLAN 三种。MAC VLAN 和协议 VLAN 仅对 untag 数据包和优先级 tag 数据包生效，当一个数据包同时满足 802.1Q VLAN、MAC VLAN 和协议 VLAN 时，交换机将按照 MAC VLAN、协议 VLAN、PVID 的顺序来处理数据包，在相应 VLAN 中转发数据包。

6.1 802.1Q VLAN

由于普通交换机工作在 OSI 模型的数据链路层，若要交换机能够识别不同 VLAN 的数据包，只能对数据包的数据链路层封装进行 VLAN 识别。因此，VLAN 识别字段被添加到数据链路层封装中。

IEEE 802.1Q协议为了标准化VLAN实现方案，对带有VLAN标识的数据包结构进行了统一规定。协议规定在目的MAC地址和源MAC地址之后封装 4 个字节的VLAN Tag，用以标识VLAN的相关信息，如图 6-2所示。VLAN Tag包含四个字段，分别是TPID（Tag Protocol Identifier，标签协议标识符）、Priority、CFI（Canonical Format Indicator，标准格式指示位）和VLAN ID。

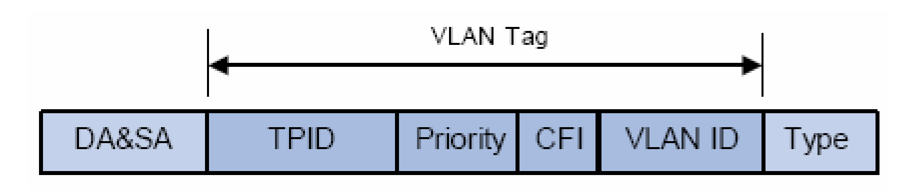


图 6-2 VLAN Tag 组成字段

1) TPID：用来表示本数据帧是带有 VLAN Tag 的数据。该字段长度为 16bit。协议规定的缺省取值为 0x8100。

2) Priority：用来表示数据包的传输优先级。

3) CFI：以太网交换机中，CFI 总被设置为 0。由于兼容特性，CFI 常用于以太网类网络和令牌环类网络之间，如果在以太网端口接收的帧 CFI 设置为 1，表示该帧不进行转发，这是因为以太网端口是一个无标签端口。

4) VLAN ID：用来标识该报文所属 VLAN 的编号。该字段长度为 12bit，取值范围为 0~4095。由于 0 和 4095 通常不使用，所以 VLAN ID 的取值范围一般为 1~4094。VLAN ID 简称 VID。

交换机利用 VLAN ID 来识别报文所属的 VLAN，当接收到的数据包不携带 VLAN Tag 时，交换机会为该数据包封装带有接收端口缺省 VLAN ID 的 VLAN Tag，将数据包在接收端口的缺省 VLAN 中进行传输。

本手册中，对包含 VLAN Tag 字段的数据包我们简称为 tag 帧，untag 帧指数据包中没有 VLAN Tag 字段的数据包，优先级 tag 帧指数据包中有 VLAN Tag 字段，但 VLAN ID 为 0 的数据包。

➢ 端口的三种链路类型

在创建 802.1Q VLAN 时，需要根据端口连接的设备设置端口的链路类型。端口的链路类型有下面三种：

1) ACCESS：端口只能属于 1 个 VLAN，出口规则为 UNTAG，多为连接用户终端设备的端口。当 ACCESS 类型端口加入了其它 VLAN 时，则自动退出原有 VLAN。

2) TRUNK：端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，常用于网络设备之间级连。在网络中 VLAN 经常跨接在不同交换机上，TRUNK 类型端口的出口规则为 TAG，能够保证转发各种 VLAN 的数据包时不改变其携带的 VLAN 信息。

3) GENERAL：端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 的报文，可以用于网络设备之间连接，也可以用于连接用户设备。GENERAL 类型端口的出口规则可以根据该端口连接设备的实际情况灵活配置。

➢ **PVID 与 VLAN 数据包处理关系**

PVID（Port VLAN ID），就是端口的缺省 VID。当交换机的端口接收到的报文不带 VLAN Tag 时，交换机会根据接收端口的 PVID 值为该报文插入 VLAN Tag，并进行转发。

当在局域网中划分 VLAN 时，PVID 是每个端口的一个重要参数，表示端口默认所属的 VLAN。它有两个用途：

1) 当端口收到 untag 报文时，将根据 PVID 为数据包插入 VLAN Tag。

2) PVID 指定了端口的默认广播域，即当端口接收到 UL 包或广播包的时候，交换机将这些数据包在该端口的缺省 VLAN 内广播。

端口的链路类型本质上是交换机对出入端口的VLAN Tag的处理方式，详细规则如表 6-1所示。

<table>
<tr><th rowspan="2">端口类型</th><th colspan="2">对接收报文的处理</th><th rowspan="2">发送报文时的处理</th></tr>
<tr><th>报文不带 Tag</th><th>报文带 Tag</th></tr>
<tr><td>Access</td><td rowspan="3">接收报文，并为报文添加缺省的 VLAN Tag 即输入端口的 PVID。</td><td>当 VID＝端口 PVID, 接收报文。
当 VID≠端口 PVID, 丢弃报文。</td><td>去掉 Tag 后，发送报文。</td></tr>
<tr><td>Trunk</td><td rowspan="2">当 VID 属于端口允许通过的 VLAN ID 时, 接收报文。
当 VID 不属于该端口允许通过的 VLAN ID 时, 丢弃报文。</td><td>保持原有 Tag 发送报文。</td></tr>
<tr><td>General</td><td>当出口规则配置为 TAG 时，保持原有 tag 发送报文。
当出口规则配置为 UNTAG 时，去 tag 后发送报文。</td></tr>
</table>

表 6-1 端口类型与 VLAN 数据处理关系

IEEE 802.1Q VLAN 功能包括 **VLAN 配置**、**端口配置**两个配置页面。

6.1.1 VLAN配置

在 VLAN 配置页面中可以查看当前已经创建的 802.1Q VLAN。

进入页面的方法：**VLAN>>802.1Q VLAN>>VLAN 配置**



图 6-3 查看 VLAN 列表

在缺省情况下，为了保证交换机在出厂情况下能正常通信，所有端口的缺省 VLAN 均为 VLAN1，只有属于 VLAN1 的端口才能访问交换机 Web 页面。VLAN1 无法编辑和删除。

条目介绍：

➢ 端口配置

VLAN ID 选择：	点击<选择>按键，可根据所输 VLAN ID，快速查找 VLAN 条目。
选择：	勾选条目进行删除，可多选。
VLAN ID：	显示 VLAN ID。
描述：	显示 VLAN 的描述信息。
端口成员：	显示 VLAN 的端口成员。

操作： 对单个 VLAN 条目进行相应操作。

- 编辑：修改 VLAN 配置。
- 查看：查看 VLAN 配置信息。

点击<编辑>按键，可以对相应的 VLAN 进行编辑。点击<新建>按键，可以创建新的 VLAN。



图 6-4 创建或编辑 802.1Q VLAN

条目介绍：

➢ **VLAN 配置**

VLAN ID： 填写 VLAN ID。

VLAN 描述： 填写 VLAN 的描述信息，以便区分各个 VLAN 的用途。

VID 检查 点击<VID 检查>按键，检查所填的 VLAN ID 是否有效。

➢ 选择端口成员

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

选择： 勾选端口配置属于 VLAN 的端口成员，可多选也可不选。

端口： 显示交换机的端口号。

链路类型： 显示相应端口的端口类型，本项可在**端口配置**页面中进行设置。

出口规则： 选择 VLAN 端口成员的出口规则。默认为 UNTAG。

- TAG：输出的数据帧带有 tag 信息。
- UNTAG：输出的数据帧不带 tag 信息。

LAG： 显示端口当前所属的汇聚组。

6.1.2 端口配置

在创建 802.1Q VLAN 时，需要对端口连接的设备进行了解，以便设置各端口的参数。

进入页面的方法：**VLAN>>802.1Q VLAN>>端口配置**



图6-5 802.1Q VLAN—端口配置

条目介绍：

> **VLAN 端口配置**

端口选择： 点击<选择>按键，可根据所输端口号，快速查找端口条目。

选择： 勾选端口配置端口类型和 PVID 值，可多选。

端口： 显示交换机的端口号。

端口类型： 选择交换机的端口类型。默认为 ACCESS。

- ACCESS：该端口只能加入一个 VLAN，出口规则为 UNTAG。PVID 值与当前 VLAN ID 的值保持相同。如果 VLAN 删除，相应端口的 PVID 会自动置为默认值 1。
- TRUNK：该端口可加入多个 VLAN，出口规则为 TAG。PVID 值可设置为当前端口加入的任意一个 VLAN 的 VID 值。
- GENERAL：该端口可加入多个 VLAN，且允许根据不同 VLAN 选择不同的出口规则，默认出口规则为 UNTAG。PVID 值可设置为当前端口加入的任意一个 VLAN 的 VID 值。

PVID： 填写交换机物理端口的 PVID 值。默认为 1。

LAG： 显示端口当前所属的汇聚组。

所属 VLAN： 查询本端口所加入的 VLAN 信息。

点击<查询>按键，可以查询相应端口所属。



图6-6 查看端口所属 VLAN

条目介绍：

➢ 端口加入的 **VLAN**

VLAN ID 查找： 点击<查找>按键，可根据所输 VLAN ID，快速查找端口所属的 VLAN 条目。

VLAN ID： 显示 VLAN ID。

VLAN 描述： 显示 VLAN 的描述信息。

从该 VLAN 移除： 点击<移除>按键，将本端口从相应 VLAN 中移除。

802.1Q VLAN 配置步骤：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面根据端口连接的设备设置端口类型。
2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。
3	编辑/查看 VLAN	可选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面点击<编辑>或<查看>按键，可以对相应的 VLAN 进行编辑和查看。
4	删除 VLAN	可选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面勾选相应的 VLAN 条目，点击<删除>按键进行删除。

6.2 MAC VLAN

MAC VLAN是VLAN的另一种划分方法，根据每个主机的MAC地址来划分VLAN，即对每个主机的MAC地址均划分到VLAN中。MAC VLAN的优点在于，将MAC地址与VLAN绑定后，该MAC地址对应的设备可以随意切换端口，只要连接到相应VLAN的成员端口即可，而不必改变VLAN成员的配置。

MAC VLAN 中数据包处理有如下特点：

1. 当端口收到 UNTAG 数据包时，首先查看是否创建配置相应的 MAC VLAN，若已创建 MAC VLAN，则给数据包插入 MAC VLAN 的 TAG；若没有相应的 MAC VLAN，则根据接收端口的 PVID 值给数据包插入 TAG，并将数据包在相应的 VLAN 中转发。
2. 当端口收到 TAG 数据包时，交换机按照 802.1Q VLAN 的方式处理该帧。如果接收端口允许该 VLAN 的数据包通过，则正常转发；如果不允许，则丢弃该数据包。
3. 将某个主机的 MAC 划分到 802.1Q VLAN 中后，为了保证该主机能够在此 VLAN 内正常通信，请将其接入端口设置成相应的 802.1Q VLAN 成员。详情请查看。

6.2.1 MAC VLAN

在 MAC VLAN 页面中，可以创建 MAC VLAN 并查看当前已创建的 MAC VLAN。

进入页面的方法：**VLAN>>MAC VLAN>>MAC VLAN**

图 6-7 创建并查看 MAC VLAN

条目介绍：

- **MAC VLAN 配置**

MAC 地址： 输入 MAC 地址。

MAC 描述： 输入对 MAC 地址的描述，以便区分各个 MAC 的用途。

VLAN ID： 输入该 MAC VLAN 对应的 VLAN ID，此 VLAN 必须是输入端口所在的 802.1Q VLAN。

- **MAC VLAN 列表**

MAC 地址选择： 点击<选择>按键，可根据所输 MAC 快速查找 MAC VLAN 条目。

选择： 勾选条目进行删除，可多选。

MAC 地址： 显示 MAC 地址。

MAC 描述： 显示此 MAC 的描述信息，以便区分各个 MAC 的设备。

VLAN ID： 显示该 MAC 对应的 VLAN ID。

操作： 点击对应条目<编辑>按键，可以修改该条目的参数。修改完毕后，点击<修改>按键，修改内容生效。

6.2.2 端口使能

端口使能用来开启端口的MAC VLAN功能。只有在配置了MAC VLAN并使能端口，才能正式启用MAC VLAN功能。

进入页面的方法：**VLAN>>MAC VLAN>>端口使能**

端口使能					
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6
☐ 7	☐ 8	☐ 9	☐ 10	☐ 11	☐ 12
☐ 13	☐ 14	☐ 15	☐ 16	☐ 17	☐ 18
☐ 19	☐ 20	☐ 21	☐ 22	☐ 23	☐ 24
☐ 25	☐ 26	☐ 27	☐ 28		

提交 全选 清空 帮助

图 6-8 开启 MAC VLAN 使能端口

勾选端口启用MAC VLAN功能，默认情况下所有端口MAC VLAN功能均已关闭。

MAC VLAN 配置步骤：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面结合实际网络结构设置端口链路类型。
2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。
3	创建 MAC VLAN	必选操作。在 **VLAN>>MAC VLAN** 页面创建 MAC VLAN。创建了 MAC VLAN 后，对应 MAC 地址的设备在交换机上的连接端口也必须是 VLAN 成员，才能保证正常通信。

6.3 协议VLAN

协议VLAN是按照网络层协议来划分VLAN，可分为IP、IPX、DECnet、AppleTalk、Banyan等VLAN网络。这种按网络层协议来组成的VLAN，可使广播域跨越多个交换机，同时用户在网络内部可以自由移动且无须改变其VLAN成员身份。对于希望针对具体应用和服务来管理用户的网络管理员，可通过划分协议VLAN来进行管理。

本交换机可针对常见的协议类型划分VLAN，常用协议类型值见下表。请根据实际需要创建协议VLAN。

协议类型	对应取值
ARP	0x0806

IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888E

表6-2 常用协议类型

协议 VLAN 中数据包处理有如下特点：

1. 当端口收到UNTAG数据包时，首先查看是否创建配置相应的协议VLAN，若已创建协议VLAN，则给数据包插入协议VLAN的TAG；若没有相应的协议VLAN，则根据接收端口的PVID值给数据包插入TAG，并将数据包在相应的VLAN中转发。
2. 当端口收到TAG数据包时，交换机按照802.1Q VLAN的方式处理该帧。如果接收端口属于携带该VLAN TAG的数据包通过，则正常转发；如果不属于，则丢弃该数据包。

划分了协议VLAN后，为了保证数据的正常传输，请将协议VLAN的使能端口设置为相应 802.1Q VLAN成员。详情请查看表 6-1 端口类型与VLAN数据处理关系。

6.3.1 协议配置

在协议配置页面中，可以创建协议VLAN并查看当前已创建的协议VLAN。

进入页面的方法：**VLAN>>协议 VLAN>>协议配置**



图 6-9 创建并查看协议 VLAN

条目介绍：

➢ 协议 **VLAN** 配置

协议类型： 选择交换机已定义的协议模板。

VLAN ID： 输入该协议 VLAN 对应的 VLAN ID，此 VLAN 必须是输入端口所在的 802.1Q VLAN。

➢ 协议 **VLAN** 列表

选择： 勾选条目进行删除，可多选。

协议类型： 显示协议 VLAN 的协议类型。

Ether Type： 显示该协议 VLAN 的以太网协议类型值。

VLAN ID： 显示该协议对应的 VLAN ID。

操作： 点击对应条目<编辑>按键，可以修改该条目的参数。修改完毕后，点击<修改>按键，修改内容生效。

6.3.2 协议模板

配置协议VLAN前应先配置协议模板，本交换机在出厂默认情况下已经定义了IP、ARP和RARP等协议模板，若需要更多的协议模板时，请在此页面中添加。

进入页面的方法：**VLAN>>协议 VLAN>>协议模板**



图 6-10 创建并查看协议模板

条目介绍：

➢ 协议模板配置

协议类型： 配置新定义的协议模板的名称。

Ether Type： 配置该协议模板中以太网协议类型值。

➢ 协议模板列表

选择： 勾选条目进行删除，可多选。

协议类型： 显示协议模板的名称。

Ether Type： 显示该协议模板中以太网协议类型值。

注意：

- 当协议模板与 VLAN 绑定后，将无法删除协议模板。

6.3.3 端口使能

端口使能用来开启端口的协议VLAN功能。只有在配置了协议VLAN并使能端口，才能正式启用协议

VLAN功能。

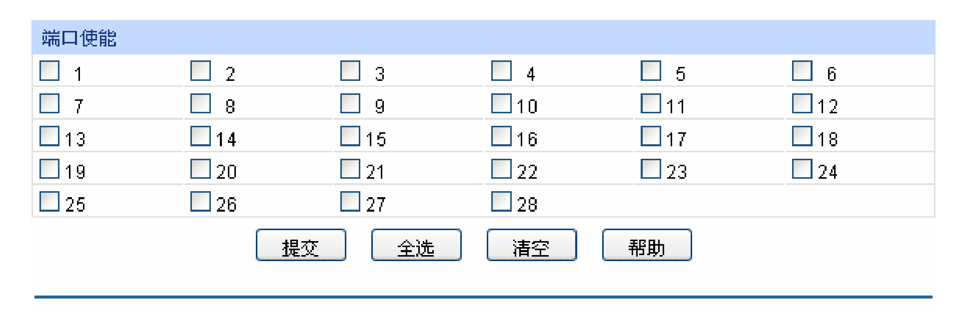


图 6-11 开启协议 VLAN 使能端口

勾选端口启用协议VLAN功能，默认情况下所有端口协议VLAN功能均已关闭。

协议 VLAN 配置步骤：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面结合实际网络结构设置端口链路类型。
2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。
3	创建协议模板	必选操作。配置协议 VLAN 前应先在 **VLAN>>协议 VLAN>>协议模板**页面配置协议模板。
4	选择支持协议 VLAN 的端口	必选操作。在 **VLAN>>协议 VLAN>>端口使能**页面选择支持协议 VLAN 的端口。
5	创建协议 VLAN	必选操作。在 **VLAN>>协议 VLAN>>协议配置**页面中选择协议类型并输入 VLAN ID 来创建 VLAN。
6	编辑/查看 VLAN	可选操作。在 **VLAN>>协议 VLAN>>协议配置**页面点击<编辑>按键对相应的 VLAN 进行编辑。
7	删除 VLAN	可选操作。在**协议配置**页面勾选相应的 VLAN 条目，点击<删除>按键进行删除。

6.4 GVRP

GVRP（GARP VLAN Registration Protocol，GARP VLAN注册协议）是GARP（Generic Attribute Registration Protocol，通用属性注册协议）的一种应用。它通过在端口动态注册和注销VLAN信息来达到创建或删除VLAN的目的，并传播VLAN信息到其它交换机中，减少配置VLAN时烦琐的手动操作。

➢ **GARP 简介**

GARP提供了一种机制，用于协助同一个局域网内的交换成员之间分发、传播和注册某种信息。GARP

本身不作为一个实体存在于设备中，遵循GARP协议的应用实体称为GARP应用，GVRP就是GARP的一种应用。当GARP应用实体存在于设备的某个端口上时，该端口称为GARP应用实体。

网络中的GARP应用实体之间通过传递GARP消息来完成相关的信息交换，GARP协议定义有三类消息，分别为Join消息、Leave消息和LeaveAll消息，三种消息完成相关属性信息的注册或注销。

Join消息：当一个GARP应用实体希望其它设备注册自己的属性信息时，它将对外发送Join消息；当收到其它实体的Join消息或本设备静态配置了某些属性，需要其它GARP应用实体进行注册时，它也会向外发送Join消息。

Leave消息：当一个GARP应用实体希望其它设备注销自己的属性信息时，它将对外发送Leave消息；当收到其它实体的Leave消息注销某些属性或静态注销了某些属性后，它也会向外发送Leave消息。

LeaveAll消息：每个GARP应用实体启动后，将同时启动LeaveAll定时器。当该定时器超时后，GARP应用实体将对外发送LeaveAll消息，LeaveAll消息用来注销所有的属性，以使其它GARP应用实体重新注册本实体上所有的属性信息。

通过消息交互，所有待注册的属性信息可以传播到同一局域网中的所有GARP应用实体。

GARP消息发送的时间间隔通过定时器来控制。GARP协议定义了四种定时器，用于控制GARP消息的发送周期：

Hold定时器：当GARP应用实体接收到其它设备发送的注册信息时，不会立即将该注册信息作为一条Join消息对外发送，而是启动Hold定时器，当该定时器超时后，GARP应用实体将此时段内收到的所有注册信息放在同一个Join消息中向外发送，从而节省带宽资源。

Join定时器：GARP应用实体可以通过将每个Join消息向外发送两次来保证消息的可靠传输，在第一次发送的Join消息没有得到回复的时候，GARP应用实体会第二次发送Join消息。两次Join消息发送之间的时间间隔用Join定时器来控制。

Leave定时器：当一个GARP应用实体希望注销某属性信息时，将对外发送Leave消息，接收到该消息的GARP应用实体启动Leave定时器，如果在该定时器超时之前没有收到Join消息，则注销该属性信息。

LeaveAll定时器：每个GARP应用实体启动后，将同时启动LeaveAll定时器，当该定时器超时后，GARP应用实体将对外发送LeaveAll消息，以使其它GARP应用实体重新注册本实体上所有的属性信息。随后再启动LeaveAll定时器，开始新的一轮循环。

- **GVRP 简介**

GVRP是GARP的一种应用。它基于GARP的工作机制，维护设备中的VLAN动态注册信息，并传播VLAN信息到其它设备中。

设备启动GVRP特性后，能够接收来自其它设备的VLAN注册信息，并动态更新本地的VLAN注册信息，包括当前的VLAN成员、这些VLAN成员可以通过哪个端口到达等；同时设备能够将本地的VLAN注册信息向其它设备传播，以便使同一局域网内所有设备的VLAN信息一致。GVRP传播的VLAN注册信息既包括本地手工配置的静态注册信息，也包括来自其它设备的动态注册信息。

在本交换机中，只有TRUNK类型端口才能作为GVRP应用实体，维护交换机的VLAN注册信息。

GVRP的端口注册模式有三种：Normal、Fixed和Forbidden，各模式描述如下：

Normal模式：允许该端口动态注册、注销VLAN，传播动态VLAN以及静态VLAN信息。

Fixed模式：禁止该端口动态注册、注销VLAN，只传播静态VLAN信息，不传播动态VLAN信息。Fixed模式的端口只允许本端口所属的静态VLAN信息通过。

Forbidden模式：禁止该端口动态注册、注销VLAN，不传播除VLAN1以外的任何的VLAN信息。Forbidden模式的端口，只允许系统默认VLAN（VLAN1）通过。

进入页面的方法：**VLAN>>GVRP**

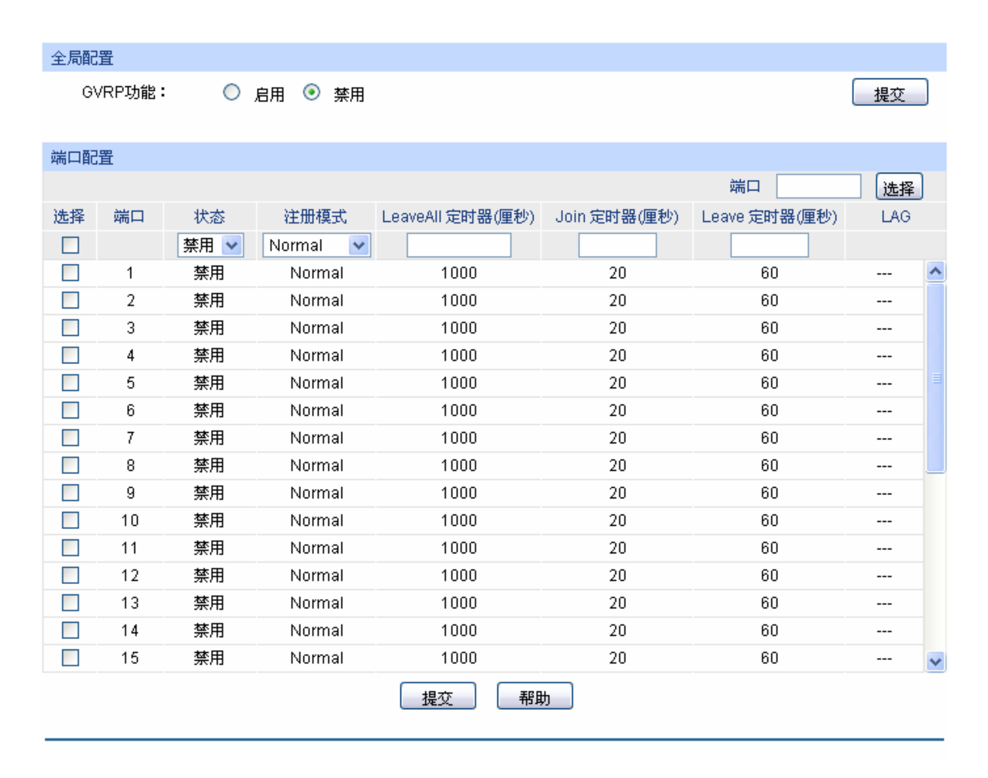


图 6-12 配置 GVRP

注 意:

- 若启用了 LAG 组成员端口的 GVRP 功能，请保持所有成员端口的状态和注册模式一致。

条目介绍：

➢ 全局配置

GVRP 功能： 选择是否启用交换机的 GVRP 功能。

➢ 端口配置

端口选择： 点击<选择>按键，可根据所输端口号快速查找相应条目。

选择： 勾选端口，配置端口 GVRP 功能参数，可多选。

端口： 显示交换机的端口号。

状态： 选择是否启用此功能。端口启用 GVRP 功能之前需要将端口类型设置为 Trunk。

注册模式： 选择端口的注册模式。

- Normal 模式：允许该端口动态注册、注销 VLAN，传播动态 VLAN 以及静态 VLAN 信息。
- Fixed：禁止该端口动态注册、注销 VLAN，只传播静态 VLAN 信息，不传播动态 VLAN 信息。
- Forbidden：禁止该端口动态注册、注销 VLAN，只允许缺省 VLAN 通过。

LeaveAll 定时器： 每个端口启动 GARP 后，同时启动 LeaveAll 定时器，端口将对外循环发送 LeaveAll 消息，以使其它端口重新注册其所有的属性信息。LeaveAll 定时器的取值范围为 1000-30000 厘秒。

Join 定时器： GARP 端口可以将每个 Join 数据包向外发送两次来保证消息的可靠传输，两次发送之间的时间间隔用 Join 定时器来控制。Join 定时器的取值范围为 20-1000 厘秒。

Leave 定时器： 接收到 Leave 数据包的 GARP 端口启动 Leave 定时器，如果在该定时器超时之前没有收到 Join 数据包，则注销相应属性信息。Leave 定时器的取值范围为 60-3000 厘秒。

LAG： 显示端口当前所属的汇聚组。

注意：

- LeaveAll 定时器要大于等于 10 倍 Leave 定时器，而 Leave 定时器要大于等于 2 倍 Join 定时器。

GVRP 配置步骤：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面将端口类型设置为 TRUNK。
2	启用 GVRP 功能	必选操作。在 **VLAN>>GVRP** 页面启用 GVRP 功能。
3	配置端口的注册模式以及各定时器时长。	必选操作。在 **VLAN>>GVRP** 页面中根据实际应用情况设置端口的参数并启用端口。

6.5 VLAN VPN

VPN（Virtual Private Network，虚拟私有网络）是随着 Internet 的广泛应用而迅速发展起来的一种新技术，用来实现在骨干网络上构建私人专用网络。通过在客户端或运营商接入端对指定报文进行处理，使骨干网络中的设备可以为其建立专用的传输隧道，保证数据的安全。

VLAN-VPN(Virtual Private Network)是一种简单、灵活的二层 VPN 技术，它通过在运营商接入端为用户的私网报文封装外层 VLAN Tag，使报文携带两层 VLAN Tag 穿越运营商网络（骨干网）。在骨干网中，报文只根据外层 VLAN Tag 进行传输，用户的私网 VLAN Tag 则当作报文中的数据部分来进行传输。

VLAN-VPN 主要可以解决如下几个问题：

（1） 为小型城域网或企业网提供一种较为简单的二层 VPN 解决方案。

（2） 缓解日益紧缺的公网 VLAN ID 资源问题。

（3） 用户可以规划自己的私网 VLAN ID，不会导致和骨干网 VLAN ID 冲突。

（4） 当运营商升级网络时，用户网络不必更改原有配置，使用户网络具有了较强的独立性。

➢ 我司交换机 VLAN-VPN 实现方式

在本交换机中，将用户的原始 VLAN 称作 C VLAN；而骨干网络中，运营商通常使用公网 VLAN 为不同的 C VLAN 提供服务，本交换机中将公网 VLAN 称为 SP VLAN。在本交换机上，需要配置 SP VLAN，然后再配置相应的 VLAN 映射，使用户的私网报文能够按照 VLAN 映射条目插入外层 Tag 或者修改 Tag，顺利穿越骨干网络到达目的地。

1. 当启用 VLAN-VPN 功能时，将同时启用 VLAN 映射功能。启用 VLAN-VPN 功能后，若端口收到 Tag 报文，交换机会根据 VLAN 映射表条目给报文封装外层 VLAN Tag，然后通过上联端口在骨干网络中传输双 Tag 报文；如果端口接收报文不带 Tag，将按照其它 VLAN 方式进行处理。

2. 如果开启了 VLAN-VPN 功能，为了保证报文能够在骨干网络中进行传输，请将连接到骨干网络的端口设置为上联端口。

3. 若不启用 VPN 模式，仅在端口使能页面使能端口，则只开启 VLAN 映射功能。当使能端口接收到 Tag 报文时，将根据 VLAN 映射表对报文中的 Tag 字段进行映射，映射到 SP VLAN 中。该功能使运营商的网络构架更为灵活，在连接接入层设备的端口上可以根据 VLAN Tag 对不同的终端用户进行分类，并在 SP VLAN 中进行传输，提供不同的网络服务。

4. 同时，本交换机还支持 TPID 值可调功能。TPID（Tag Protocol Identifier，标签协议标识）是 VLAN Tag 中的一个字段，IEEE802.1Q 协议规定该字段的取值为 0x8100。本交换机缺省采用协议规定的 TPID 值（0x8100）。某些厂商将网络设备可识别的 TPID 值设置为 0x9100 或其它数值。为了和这些设备兼容，本交换机提供了全局的 VLAN-VPN 报文 TPID 值可调功能，用户可以自行配置 TPID 值。VLAN-VPN 上联端口在转发报文时会将报文外层 VLAN Tag 中的 TPID 值替换为设定值再进行发送，从而使发送到骨干网中的 VLAN-VPN 报文可以被其它厂商的设备识别。

   由于TPID字段在以太网报文中的位置与不带VLAN Tag的报文中协议类型字段所处位置相同，为避免网络中报文转发和接收造成混乱，用户在配置VLAN-VPN时，请勿配置TPID为表6-3中列举的常用协议类型值。

协议类型	对应取值
ARP	0x0806
IP	0x0800
MPLS	0x8847/0x8848
IPX	0x8137
IS-IS	0x8000
LACP	0x8809
802.1X	0x888E

表6-3 常用以太网数据包协议类型值

本功能包括 VPN 配置、VLAN 映射和端口使能三个配置页面。

6.5.1 VPN配置

在 VPN 配置页面中，可以启用交换机 VPN 功能、设置全局 TPID 值和启用上联端口。启用 VPN 模式后，交换机将根据 VLAN 映射表条目对收到的 tag 数据包插入外层 tag。

进入页面的方法：**VLAN>>VLAN VPN>>VPN 配置**

VPN全局配置

VPN模式： ○启用 ◉禁用

全局TPID： 8100 （4位十六进制整数） 提交

VPN上联端口

☐ 1(LAG1)	☐ 2(LAG1)	☐ 3	☐ 4	☐ 5	☐ 6
☐ 7	☐ 8	☐ 9	☐ 10	☐ 11(LAG7)	☐ 12
☐ 13(LAG7)	☐ 14	☐ 15(LAG7)	☐ 16	☐ 17(LAG7)	☐ 18
☐ 19	☐ 20	☐ 21	☐ 22	☐ 23	☐ 24
☐ 25	☐ 26	☐ 27	☐ 28		

提交 全选 清空 帮助

图 6-13 VPN 全局功能配置

条目介绍：

➢ **VPN 全局配置**

VPN 模式：	选择是否启用 VLAN-VPN 功能。
全局 TPID：	填写全局 TPID。

➢ **VPN 上联端口**

勾选端口设置为 VPN 上联端口，请将连接到骨干网络的端口设置为上联端口。



注 意：

- 启用 VPN 模式后，请在 VLAN 映射功能页面创建 VLAN 映射条目。

6.5.2 VLAN映射

VLAN 映射功能可以将报文的 VLAN TAG 按照 VLAN 映射条目替换成 SP VLAN 的 VLAN TAG，然后在 SP VLAN 范围中转发报文。如果启用 VPN 模式，则按照 VLAN 映射条目对 TAG 报文插入外层 TAG，然后在新的 VLAN 中转发报文。

进入页面的方法：**VLAN>>VLAN VPN>>VLAN 映射**

VLAN映射配置

C VLAN： （1-4094）

SP VLAN： （1-4094）

描述： （1-15个字符）

添加 清空

VLAN映射列表

C VLAN 选择

选择	C VLAN	SP VLAN	描述	操作
当前VLAN映射列表为空				

全选 删除 帮助

图 6-14 创建 VLAN 映射条目

条目介绍：

➢ **VLAN 映射配置**

C VLAN： Customer VLAN（用户 VLAN）。本交换机中收到 TAG 报文时，对接收报文所属的 VLAN 称为 C VLAN。

SP VLAN： Service Provider VLAN（服务商 VLAN）。在骨干网络中，用户可以使用公网 VLAN 为不同的 C VLAN 提供服务，本交换机中将公网 VLAN 称为 SP VLAN。

描述： 填写 VLAN 映射条目的附加描述信息，可留空。

➢ **VLAN 映射列表**

C VLAN 选择： 点击<选择>按键，可根据所输的 C VLAN 快速查找 VLAN 映射条目。

选择： 勾选条目进行删除，可多选。

操作： 点击对应条目<编辑>按键，可以修改该条目的参数。修改完毕后，点击<修改>按键，修改内容生效。

6.5.3 端口使能

端口使能用来开启端口的VLAN映射功能。只有在配置了VLAN映射后并使能端口，才能正式启用VLAN映射功能。

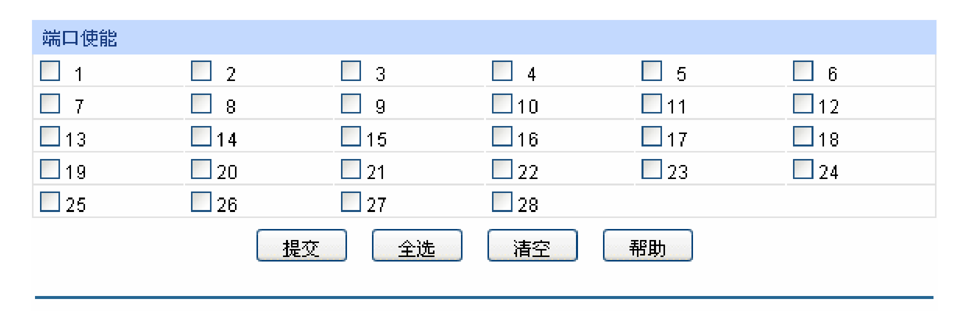


图 6-15 开启 VLAN 映射使能端口

勾选端口启用VLAN映射功能，默认情况下关闭所有端口的VLAN映射功能。

注意：

- 启用 VPN 模式时无需配置端口使能。当未启用 VPN 模式时，端口使能对 VLAN 映射功能生效。

VLAN VPN 配置步骤：

步骤	操作	说明
1	启用 VPN 模式	必选操作。在 **VLAN>>VLAN VPN>>VPN 配置**功能页面启用 VPN 模式功能。
2	设置全局 TPID	可选操作。在 **VLAN>>VLAN VPN>>VPN 配置**功能页面，根据上联端口的对端设备属性设置全局 TPID 值。
3	设置上联端口	必选操作。在 **VLAN>>VLAN VPN>>VPN 配置**功能页面启用 VPN 上联端口，请将连接到骨干网络的端口设置为上联端口。
4	创建 VLAN 映射条目	必选操作。在 **VLAN>>VLAN VPN>>VLAN 映射**功能页面中根据实际应用情况设置 VLAN 映射条目。
5	创建 SP VLAN	可选操作。在**VLAN>>802.1Q VLAN**功能中创建SP VLAN，创建VLAN步骤请参考802.1Q VLAN。

VLAN 映射功能配置步骤：

步骤	操作	说明
1	创建 VLAN 映射条目	必选操作。在 **VLAN>>VLAN VPN>>VLAN 映射**功能页面中根据实际应用情况设置 VLAN 映射条目。
2	设置 VLAN 映射使能端口	必选操作。在 **VLAN>>VLAN VPN>>端口使能**功能页面中选择启用 VLAN 映射功能的端口。
3	创建 SP VLAN	可选操作。在**VLAN>>802.1Q VLAN**功能中创建SP VLAN，创建VLAN步骤请参考802.1Q VLAN。

6.6 Private VLAN

Private VLAN 功能采用了分层结构，将多个 Secondary VLAN 与一个 Primary VLAN 组成 VLAN 对，下层用户通过 Secondary VLAN 相互之间进行二层报文隔离，上层设备仅需识别 Primary VLAN 从而节约了 VLAN 资源，解决了上次设备 VLAN 资源短缺以及传统 VLAN 中的广播问题。

在园区网和企业接入网中，为了保证用户信息安全，要求对各接入用户进行认证接入并相互隔离，通过VLAN进行隔离是最常见的隔离方式。随着接入用户的数量日益增长，用传统VLAN的隔离方式将消耗大量的VLAN资源，上层设备为了识别所有的VLAN，不得不建立数量庞大的VLAN。然而，根据IEEE 802.1Q协议标准定义的4个字节的VLAN Tag，其中12bits用于表示VLAN ID，这也就限制的网络设备可识别的VLAN数最多为4094个。在VLAN资源消耗殆尽的情况下，Private VLAN功能应运而生，常用网络模型如下图 6-16示。

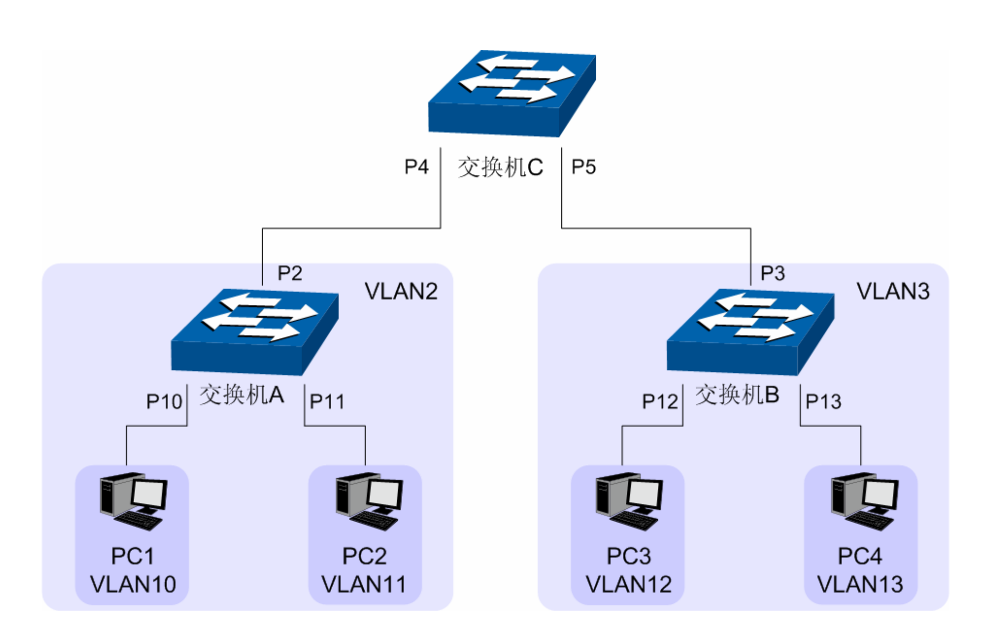


图 6-16 Private VLAN网络模型

在图 6-16中，交换机A和交换机B分别运用Private VLAN功能，建立Secondary VLAN将各PC相互隔离，并将Secondary VLAN与Primary VLAN组成VLAN对，上层设备交换机C只需识别Primary VLAN。

Private VLAN功能主要有如下有点：

（1） 解决上层设备 VLAN 资源短缺的问题。

（2） 通过 MAC 地址复制技术，将 Secondary VLAN 与 Primary VLAN 中学习到的 MAC 地址自动复制到对方 VLAN 中，可有效抑制各 VLAN 中广播通信，从而节约带宽资源，增强网络安全性。

➢ **我司交换机的 Private VLAN 实现方式**

Private VLAN 功能基于 802.1Q VLAN 建立 Primary VLAN 和 Secondary VLAN 的包含关系，通过这种包含关系，上联设备只需识别 Primary VLAN 信息，下联设备只需识别 Secondary VLAN 信息。

Primary VLAN： 上行设备感知的用户 VLAN，不是用户真正所属的 VLAN，一个 Primary VLAN 可以和多个 Secondary VLAN 建立包含关系，用于转发上层设备和 Secondary VLAN 之间的通信数据。

Secondary VLAN： 用户真正属于的 VLAN，将用户划分到不同的 Secondary VLAN 中，从而用户之间相互隔离。

根据 VLAN 特性，Primary VLAN 和 Secondary VLAN 之间也相互隔离，为了使数据在本层设备上能够正常转发，需要进一步制定严谨的端口数据处理规则以及 MAC 地址复制规则。在 Private VLAN 中有两种端口类型，Promiscuous 和 Host，详细定义和作用如下。

Promiscuous： 上行端口，和上层设备相连，负责和上行设备通信。所有添加到 Private VLAN 中的 Promiscuous 端口，将同步到 Primary VLAN 和 Secondary VLAN 中成为 VLAN 成员端口。为了向上层设备屏蔽 Secondary VLAN 的信息，Promiscuous 端口的出口规则默认为 UNTAG，可修改。当 Promiscuous 端口用于设备间的级联时，就需要把端口出口规则改为 tag。Promiscuous 端口只能作为一个 Primary VLAN 的上行端口，其 PVID 为 Primary VLAN ID，学习

到的 MAC 地址将复制到其关联的所有 Secondary VLAN 中。

Host：下行端口，和下层设备相连，负责和下行设备通信。所有添加到 Private VLAN 中的 Host 端口，将同步到 Primary VLAN 和 Secondary VLAN 中成为 VLAN 成员端口。为了向下层设备屏蔽 Primary VLAN 的信息，Host 端口的出口规则为 UNTAG。Host 端口只能加入一个 Secondary VLAN，其 PVID 为 Secondary VLAN ID，学习到的 MAC 地址将复制到关联的 Primary VLAN 中。

如图 6-16示，以图中的交换机A为例介绍我司交换机的Private VLAN功能，以下为功能配置要点。

（1） 交换机 A 建立 Private VLAN 2/10（Primary VLAN 为 VLAN 2，Secondary VLAN 为 VLAN10，下面格式同此处）和 Private VLAN 2/11。

（2） 交换机 A 的端口 10 和端口 11 作为 Host 类型端口连接终端用户，分别加入不同的 Private VLAN，通过不同的 Secondary VLAN 相互之间进行隔离。端口 2 作为 Promiscuous 类型端口连接上层设备，通过 Primary VLAN 2 向上层设备屏蔽本交换机上的 Secondary VLAN 的信息。

（3） 交换机 A 内部执行端口同步机制。创建了 Private VLAN 2/10 和 Private VLAN 2/11 后，端口 10 和端口 11 同时成为 Primary VLAN 2 的成员端口，端口出口规则为 UNTAG，端口 PVID 为各自所属的 Secondary VLAN；端口 2 连接上层设备，同时也同步到 Secondary VLAN 中成为 VLAN 成员端口，出口规则为 UNTAG，PVID 为 Primary VLAN ID。

（4） 交换机 A 内部执行 MAC 地址复制机制，解决了传统 VLAN 中常见的广播问题，以下两个表格是 MAC 地址复制前后的地址表内容。

序号	目的 MAC	VLAN	出端口
1	PC1	10	10
2	PC2	11	11
3	交换机 C	2	2

表6-4 MAC 地址复制前的地址表

序号	目的 MAC	VLAN	出端口
1	PC1	10	10
2	PC1	2	10
3	PC2	11	11
4	PC2	2	11
5	交换机 C	2	2
6	交换机 C	10	2
7	交换机 C	11	2

表6-5 MAC 地址复制后的地址表

由上表可知，在 Primary VLAN 和 Secondary VLAN 中学习到的 MAC 地址相互复制，大量消除了 VLAN 中因目的 MAC 地址未知而产生的广播问题。

本功能配置简单，包括 PVLAN 配置和端口配置两个配置页面。

6.6.1 PVLAN配置

在 PVLAN 配置页面中，可以创建 Private VLAN，将 Primary VLAN 和 Secondary VLAN 关联。

进入页面的方法：**VLAN>>Private VLAN>>PVLAN 配置**

Private VLAN 创建

Primary VLAN： （2-4094）

Secondary VLAN： （格式:2,4-5,8） 添加

查找条目

查找选项： 全部 查找

Private VLAN 列表

选择	Primary VLAN	Secondary VLAN	端口成员
☐			
☐	2	10	5
☐	2	20	
☐	3	100	3,8
☐	3	200	3

提交 删除 帮助

当前Private VLAN总数:4

注意：

为避免响应时间过长，建议每次创建Private VLAN数少于10个。

图 6-17 PVLAN 配置

条目介绍：

- **Private VLAN 创建**

  Primary VLAN： 填写 Primary VLAN ID。一个 Primary VLAN 可以和多个 Secondary VLAN 关联组成多个 Private VLAN。

  Secondary VLAN： 填写 Secondary VLAN ID。一个 Secondary VLAN 中只能和一个 Primary VLAN 关联，即加入一个 Private VLAN。

- 查找条目

  查找选项： 当创建的 Private VLAN 数过多时，可通过指定的 Primary VLAN 或 Secondary VLAN 查找相应的 Private VLAN 条目。

- **Private VLAN 列表**

  选择： 勾选条目进行删除或修改交换机 Private VLAN 配置信息，可多选。

  Primary VLAN： 显示 Private VLAN 的 Primary VLAN ID。

  Secondary VLAN： 显示 Private VLAN 的 Secondary VLAN ID。

  端口成员： 显示 Private VLAN 的成员端口。当在 Private VLAN 列表区中修改 Private VLAN 参数时，其原有的成员端口参数将失效，请重新配置。

注意：

- 在创建 Private VLAN 时，交换机可能会产生大量的地址复制，为了避免交换机响应时间过长，建议每次创建的 Private VLAN 数少于 10 个。

6.6.2 端口配置

在本页面中，可以根据端口在网络中的连接状态配置端口类型，并将端口添加到 Private VLAN 中。

进入页面的方法：**VLAN>>Private VLAN>>端口配置**

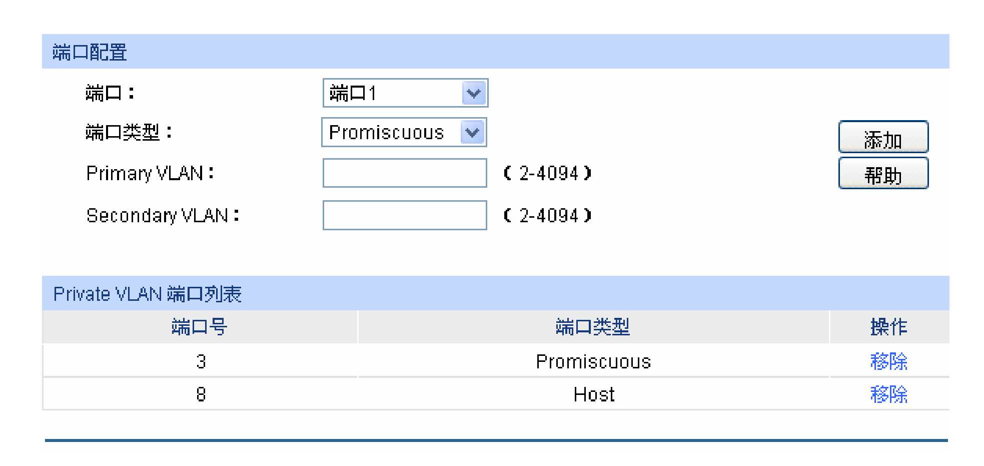


图 6-18 端口配置

条目介绍：

➢ 端口配置

端口：	选择需配置的端口号。
端口类型：	选择端口类型。 ● Promiscuous：和上行设备相连，负责和上行设备通信。 ● Host：和下行设备相连，负责和下行设备通信。
Primary VLAN：	填写该端口加入的 Primary VLAN。
Secondary VLAN：	填写该端口加入的 Secondary VLAN。

➢ **Private VLAN** 端口列表

端口号：	显示 Private VLAN 的端口号。
端口类型：	显示端口在 Private VLAN 中的端口类型。
操作：	删除 Private VLAN 的成员端口。

注意：

- 如果需要把 Promiscuous 端口加入多个 Private VLAN 中且 Primary VLAN 相同时,只需把 Promiscuous 端口加入任意一个 Private VLAN 即可，端口将自动同步到其他 Private VLAN。

Private VLAN 配置步骤：

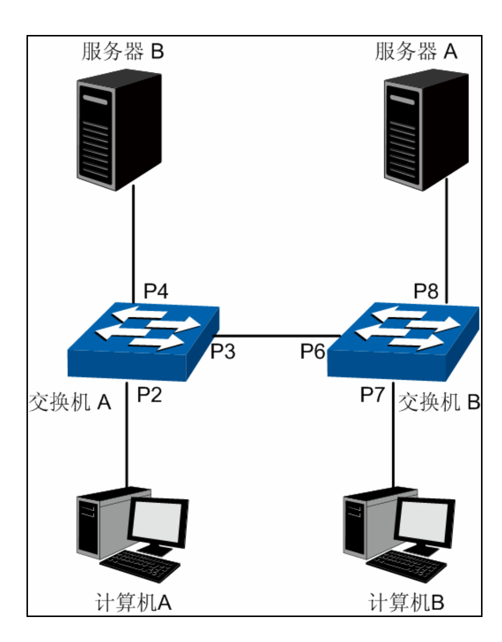
步骤	操作	说明
1	创建 Private VLAN	必选操作。在 **VLAN>>Private VLAN>>PVLAN 配置**功能页面创建 Private VLAN。
2	配置成员端口	必选操作。在 **VLAN>>Private VLAN>>端口配置**功能页面，根据端口的对端设备属性将端口添加到 Private VLAN 中。

6.7 802.1Q VLAN功能的组网应用

➢ 组网需求

- 交换机 A 连接了计算机 A 和服务器 B；
- 交换机 B 连接了计算机 B 和服务器 A；
- 计算机 A 和服务器 A 同属于一个部门；
- 计算机 B 和服务器 B 同属于一个部门；
- 两个部门以 VLAN 划分，相互之间不能通信。

➢ 组网图



图中的“P 数字”表示交换机的端口号。

➢ 配置步骤

- 配置交换机 A：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 2 的类型为 ACCESS；设置端口 3 的类型为 TRUNK；端口 4 类型为 ACCESS。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，并包含的端口 2 和端口 3。

3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，并包含的端口 3 和端口 4。

- 配置交换机 B：

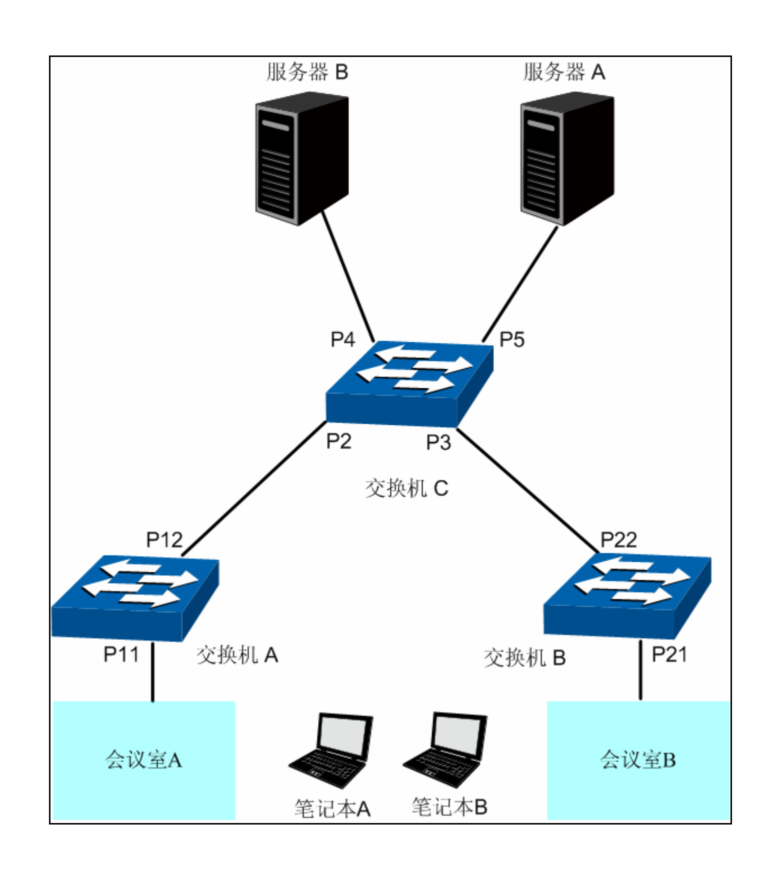
步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 7 的类型为 ACCESS；设置端口 6 的类型为 TRUNK；端口 8 类型为 ACCESS。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，并包含的端口 6 和端口 8。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，并包含的端口 6 和端口 7。

6.8 MAC VLAN功能的组网应用

- 组网需求

- 交换机 A 和交换机 B 分别连接到两个会议室，会议室为各部门共用；
- 笔记本 A 和笔记本 B 为会议室专用电脑，分别属于不同部门；
- 两个部门分别属于 VLAN10 和 VLAN20。现要求这两台笔记本电脑无论在哪个会议室使用，均只能访问自己部门的服务器，即服务器 A 和服务器 B；
- 笔记本 A 和笔记本 B 的 MAC 地址分别为 00-19-56-8A-4C-71、00-19-56-82-3B-70。

- 组网图



图中的“P 数字”表示交换机的端口号。

➢ **配置步骤**

● 配置交换机 A：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 11 的端口类型为 GENERAL，端口 12 的端口类型为 TRUNK。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，包含的端口 11 和端口 12，端口 11 的出口规则设置为 Untag。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，包含的端口 11 和端口 12，端口 11 的出口规则设置为 Untag。
4	设置 MAC VLAN 10	在 **VLAN>>MAC VLAN** 页面创建 MAC VLAN10，关联的 MAC 地址为 00-19-56-8A-4C-71。
5	设置 MAC VLAN 20	在 **VLAN>>MAC VLAN** 页面创建 MAC VLAN20，关联的 MAC 地址为 00-19-56-82-3B-70。

● 配置交换机 B：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 21 的端口类型为 GENERAL，端口 22 的端口类型为 TRUNK。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，包含的端口 21 和端口 22，端口 21 的出口规则设置为 Untag。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，包含的端口 21 和端口 22，端口 21 的出口规则设置为 Untag。
4	设置 MAC VLAN 10	在 **VLAN>>MAC VLAN** 页面创建 MAC VLAN10，关联的 MAC 地址为 00-19-56-8A-4C-71。
5	设置 MAC VLAN 20	在 **VLAN>>MAC VLAN** 页面创建 MAC VLAN20，关联的 MAC 地址为 00-19-56-82-3B-70。

● 配置交换机 C：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 2 和端口 3 的端口类型为 GENERAL，端口 4 和端口 5 的端口类型为 ACCESS。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，包含的端口 2、端口 3 和端口 5。

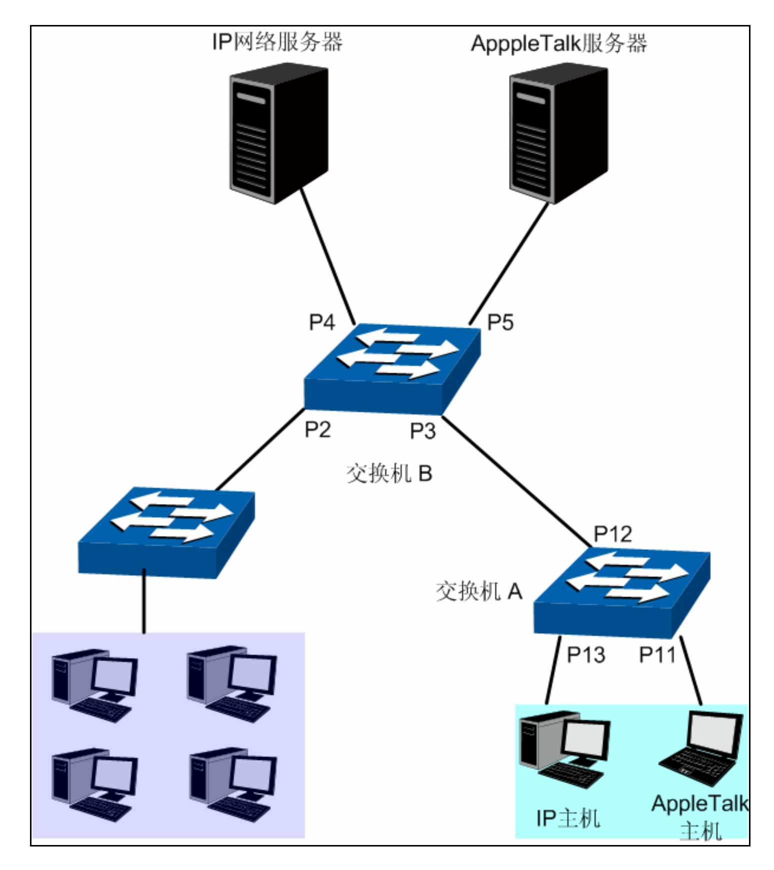
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，包含的端口 2、端口 3 和端口 4。

6.9 协议 VLAN功能的组网应用

➢ 组网需求

- 平面部门通过内部交换机 A 的端口 12 连入公司局域网；
- 平面部门中分别有 IP 主机和 AppleTalk 主机；
- IP 主机需要 IP 网络服务器提供服务，属于 VLAN10；AppleTalk 主机需要 AppleTalk 服务器提供服务，属于 VLAN20；
- 交换机 A 分别连接了 IP 网络服务器和 AppleTalk 网络服务器；

➢ 组网图



图中的“P 数字”表示交换机的端口号。

➢ 配置步骤

- 配置交换机 A：

步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 11 和端口 13 的端口类型为 ACCESS，端口 12 的端口类型为 GENERAL。

2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，包含的端口 12 和端口 13，端口 12 的出口规则设置为 Untag。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，包含的端口 11 和端口 12，端口 12 的出口规则设置为 Untag。

- 配置交换机 B：

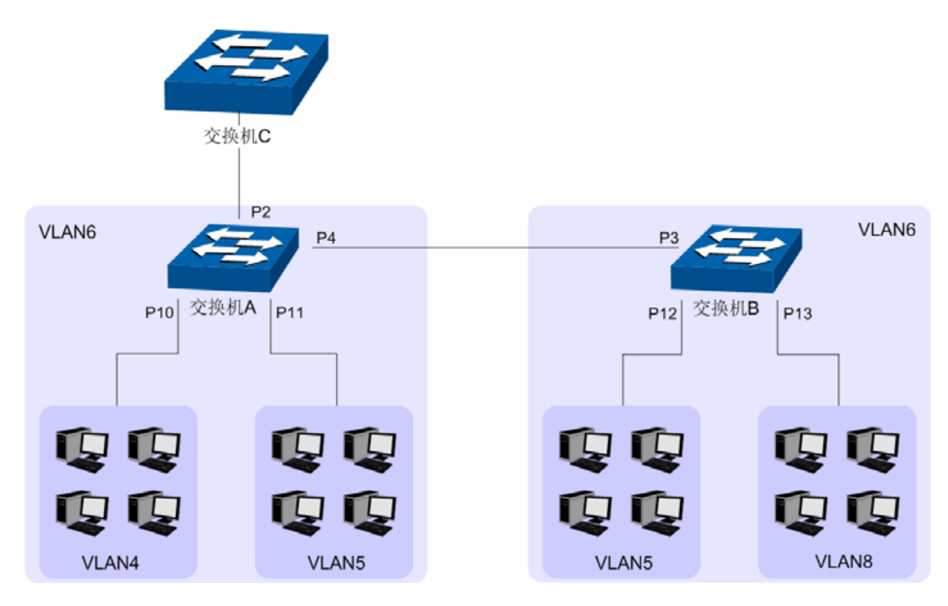
步骤	操作	说明
1	设置端口类型	必选操作。在 **VLAN>>802.1Q VLAN>>端口配置**页面设置端口 4 和端口 5 的端口类型为 ACCESS，端口 3 的端口类型为 GENERAL。
2	创建 VLAN10	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 10，包含的端口 3 和端口 4，端口 3 的出口规则设置为 Tag。
3	创建 VLAN20	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，VLAN ID 为 20，包含的端口 3 和端口 5，端口 3 的出口规则设置为 Tag。
4	创建协议模板	必选操作。此处请根据实际情况在 **VLAN>>协议 VLAN>>协议模板**页面配置协议模板。例如 IP 网络数据包以 Ethernet II 类型封装，Ether Type 字段为 0800；AppleTalk 网络数据包以 SNAP 类型封装，PID 字段为 809B。
5	设置协议 VLAN 10	在 **VLAN>>协议 VLAN>>协议组列表**页面中点击<新建>按键来创建协议 VLAN10，关联 IP 协议，并勾选成员端口 3。
6	设置协议 VLAN 20	在 **VLAN>>协议 VLAN>>协议组列表**页面中点击<新建>按键来创建协议 VLAN20，关联 AppleTalk 协议，并勾选成员端口 3。

6.10 Private VLAN功能的组网应用

> 组网需求

- ISP 向某公司提供了网络接入服务，连接到 ISP 机房的接入交换机 A 上，并通过 VLAN6 向企业提供网络服务；
- 企业中心交换机上连接了许多用户，各用户之间要求通过 VLAN 功能进行二层隔离；
- 中心交换机向下级联了另外一台汇聚层交换机，汇聚层交换机上配置了 VLAN 功能，部分 VLAN 要求和中心交换机上的 VLAN 进行连通，且所连接的用户均能够访问网络。

> 组网图



图中的“P 数字”表示交换机的端口号。

➢ **配置步骤**

● 配置交换机 A：

步骤	操作	说明
1	创 建 Private VLAN	必选操作。在 **VLAN>>Private VLAN>>PVLAN 配置**页面设置创建 Private VLAN 6/4 和 Private VLAN 6/5。
2	为 Private VLAN 添加端口	必选操作。在 **VLAN>>Private VLAN>>端口配置**页面，配置端口 10 的端口类型为 Host 并添加到 Private VLAN 6/4 中；配置端口 11 的端口类型为 Host 并添加到 Private VLAN 6/5 中；配置端口 2 和端口 4 的端口类型为 Promiscuous 并添加到 Private VLAN 6/4 中。
3	配置端口出口规则	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面，编辑各 VLAN 端口的出口规则，P4 作为交换机之间的级联，要求在 Private VLAN 中的出口规则为 Tag。

● 配置交换机 B：

步骤	操作	说明
1	创 建 Private VLAN	必选操作。在 **VLAN>>Private VLAN>>PVLAN 配置**页面设置创建 Private VLAN 6/5 和 Private VLAN 6/8。
2	为 Private VLAN 添加端口	必选操作。在 **VLAN>>Private VLAN>>端口配置**页面，配置端口 12 的端口类型为 Host 并添加到 Private VLAN 6/5 中；配置端口 13 的端口类型为 Host 并添加到 Private VLAN 6/8 中；配置端口 3 的端口类型为 Promiscuous 并添加到 Private VLAN 6/5 中。
3	配置端口出口规则	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面，编辑各 VLAN 端口的出口规则，P3 作为交换机之间的级联，要求在 Private VLAN 中的出口规则为 Tag。

回目录

第7章 生成树

STP（Spanning Tree Protocol，生成树协议）是根据 IEEE 802.1D 标准建立的，用于在局域网中消除数据链路层物理环路的协议。运行该协议的设备通过彼此交互信息发现网络中的环路，并有选择的对某些端口进行阻塞，最终将环路网络结构修剪成无环路的树型网络结构，从而防止报文在环路网络中不断增生和无限循环，避免设备由于重复接收相同的报文所造成的报文处理能力下降的问题发生。

STP 采用的协议报文是 BPDU（Bridge Protocol Data Unit，桥协议数据单元），也称为配置消息，BPDU 中包含了足够的信息来保证设备完成生成树的计算过程。STP 即是通过在设备之间传递 BPDU 来确定网络的拓扑结构。

➢ **BPDU 格式及字段说明**

要实现生成树的功能，交换机之间传递 BPDU 报文实现信息交互，所有支持 STP 协议的交换机都会接收并处理收到的报文。该报文在数据区里携带了用于生成树计算的所有有用信息。

标准生成树的 BPDU 帧格式及字段说明：

2	1	1	1	8	4
Protocol Identifier	Version	Message Type	Flag	Root ID	Root Path Cost
Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay
8	2	2	2	2	2

Protocol identifier： 协议标识

Version： 协议版本

Message type： BPDU 类型

Flag： 标志位

Root ID： 根桥 ID，由两字节的优先级和 6 字节 MAC 地址构成

Root path cost： 根路径开销

Bridge ID： 桥 ID，表示发送 BPDU 的桥的 ID，由 2 字节优先级和 6 字节 MAC 地址构成

Port ID： 端口 ID，标识发出 BPDU 的端口

Message age： BPDU 生存时间

Maximum age： 当前 BPDU 的老化时间，即端口保存 BPDU 的最长时间

Hello time： 根桥发送 BPDU 的周期

Forward delay： 表示在拓扑改变后，交换机在发送数据包前维持在监听和学习状态的时间

➢ **STP 的基本概念**

桥 ID（Bridge Identifier）：桥 ID 是桥的优先级和其 MAC 地址的综合数值，其中桥优先级是一个可以设定的参数。桥 ID 越低，则桥的优先级越高，这样可以增加其成为根桥的可能性。

根桥（Root Bridge）：具有最小桥 ID 的交换机是根桥。请将环路中所有交换机当中最好的一台设置为根桥交换机，以保证能够提供最好的网络性能和可靠性。

指定桥（Designated Bridge）：在每个网段中，到根桥的路径开销最低的桥将成为指定桥，数据包将通过它转发到该网段。当所有的交换机具有相同的根路径开销时，具有最低的桥 ID 的交换机会被选为指定桥。

根路径开销（Root Path Cost）：一台交换机的根路径开销是根端口的路径开销与数据包经过的所有交换机的根路径开销之和。根桥的根路径开销是零。

桥优先级（Bridge Priority）：是一个用户可以设定的参数，数值范围从 0 到 61440。设定的值越小，优先级越高。交换机的桥优先级越高，才越有可能成为根桥。

根端口（Root Port）：非根桥的交换机上离根桥最近的端口，负责与根桥进行通信，这个端口到根桥的路径开销最低。当多个端口具有相同的到根桥的路径开销时，具有最高端口优先级的端口会成为根端口。

指定端口（Designated Port）：指定桥上向本交换机转发数据的端口。

端口优先级（Port Priority）：数值范围从 0 到 255，值越小，端口的优先级就越高。端口的优先级越高，才越有可能成为根端口。

路径开销（Path Cost）：STP 协议用于选择链路的参考值。STP 协议通过计算路径开销，选择较为“强壮”的链路，阻塞多余的链路，将网络修剪成无环路的树型网络结构。

生成树基本概念的组网示意图如图 7-1所示。交换机A、B、C三者顺次相连，经STP计算过后，交换机A被选为根桥，端口 2 和端口 6 之间的线路被阻塞。

- 桥：交换机 A 为整个网络的根桥；交换机 B 是交换机 C 的指定桥。
- 端口：端口 3 和端口 5 分别为交换机 B 和交换机 C 的根端口；端口 1 和端口 4 分别为交换机 A 和交换机 B 的指定端口；端口 6 为交换机 C 的阻塞端口。

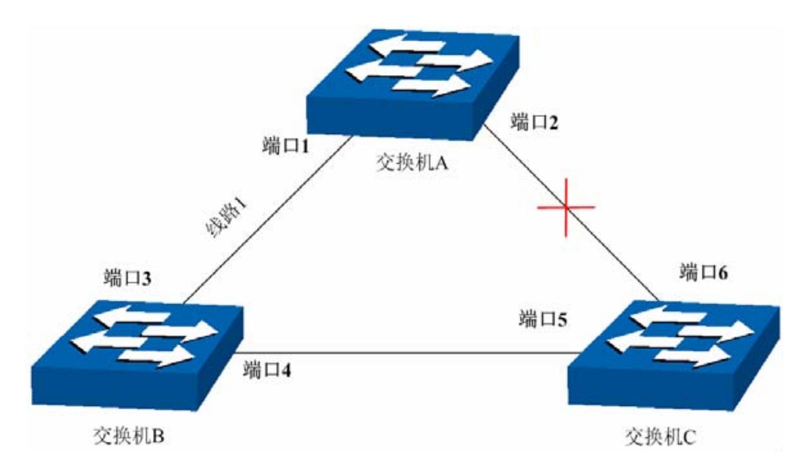


图 7-1 生成树基本概念组网图

➢ **STP 定时器**

联络时间（Hello Time）：

数值范围从 1 秒到 10 秒。是指根桥向其它所有交换机发出 BPDU 数据包的时间间隔，用于交换机检测链路是否存在故障。

老化时间（Max. Age）：

数值范围从 6 秒到 40 秒。如果在超出老化时间之后，还没有收到根桥发出的 BPDU 数据包，那么交换机将向其它所有的交换机发出 BPDU 数据包，重新计算生成树。

传输时延（Forward Delay）：

数值范围从 4 秒到 30 秒。是指交换机的端口状态迁移所用的时间。

当网络故障引发生成树重新计算时，生成树的结构将发生相应的变化。但是重新计算得到的新配置消息无法立刻传遍整个网络，如果端口状态立刻迁移的话，可能会产生暂时性的环路。为此，生成树协议采用了一种状态迁移的机制，新的根端口和指定端口开始数据转发之前要经过 2 倍的传输时延，这个延时保证了新的配置消息已经传遍整个网络。

- **STP 模式的 BPDU 的优先级比较原则**

假定有两条 BPDU X 和 Y，则：

如果 X 的根桥 ID 小于 Y 的根桥 ID，则 X 优于 Y

如果 X 和 Y 的根桥 ID 相同，但 X 的根路径开销小于 Y，则 X 优于 Y

如果 X 和 Y 的根桥 ID 和根路径开销相同，但 X 的桥 ID 小于 Y，则 X 优于 Y

如果 X 和 Y 的根桥 ID、根路径开销和桥 ID 相同，但 X 的端口 ID 小于 Y，则 X 优于 Y

- **STP 的计算过程**

  - 初始状态

每台交换机在初始时会生成以自己为根桥的 BPDU，根路径开销为 0，指定桥 ID 为自身设备 ID，指定端口为本端口。

  - 最优 BPDU 的选择

每台交换机都向外发送自己的 BPDU，同时也会收到其它交换机发送的 BPDU。比较过程如下表所述：

步骤	内容
1	当端口收到的BPDU比本端口BPDU的优先级低时，交换机将丢弃接收到的BPDU，保留该端口的 BPDU；否则，交换机将接收到的 BPDU 替换成为该端口的 BPDU。
2	交换机将所有端口的 BPDU 进行比较，选出最优的 BPDU 作为本交换机的 BPDU。

表 7-1 最优 BPDU 的选择

  - 根桥的选择

通过交换配置消息，设备之间比较根桥 ID，网络中根桥 ID 最小的设备被选为根桥。

  - 根端口、指定端口的选择

根端口、指定端口的选择过程如下表所述：

步骤	内容
1	非根桥交换机将接收到最优 BPDU 的那个端口指定为根端口。

2	交换机根据根端口的BPDU和根端口的路径开销，为其它端口计算一个端口BPDU： • 根桥 ID 替换为根端口的根桥 ID； • 根路径开销替换为根端口的根路径开销加上本端口到根端口的路径开销； • 指定桥 ID 替换为自身设备的 ID； • 指定端口 ID 替换为自身端口 ID。
3	交换机使用计算出来的 BPDU 和需要确定端口角色的端口上的 BPDU 进行比较，并根据比较结果进行不同的处理： • 如果计算出来的 BPDU 优，则设备就将该端口定为指定端口，端口上的 BPDU 被计算出来的 BPDU 替换，并周期性向外发送。 • 如果端口上的 BPDU 优，则设备不更新该端口 BPDU 并将此端口阻塞，该端口将不再转发数据，只接收但不发送配置消息；

表 7-2 根端口、指定端口的选择

说明：

- 在拓扑稳定状态，只有根端口和指定端口转发数据，其它的端口都处于阻塞状态，它们只接收 BPDU 报文而不转发数据。

➢ **RSTP**

RSTP（Rapid Spanning Tree Protocol，快速生成树协议）是优化版的 STP，它大大缩短了端口进入转发状态的延时，从而缩短了网络最终达到拓扑稳定所需要的时间。RSTP 的端口状态实现快速迁移的前提如下：

- 根端口的端口状态快速迁移的条件是：本设备上旧的根端口已经停止转发数据，而且上游指定端口已经开始转发数据。
- 指定端口的端口状态快速迁移的条件是：指定端口是边缘端口或者指定端口与点对点链路相连。如果指定端口是边缘端口，则指定端口可以直接进入转发状态；如果指定端口连接着点对点链路，则设备可以通过与下游设备握手，得到响应后即刻进入转发状态。

➢ **RSTP 的基本概念**

边缘端口（Edge Port）：直接与终端相连而不是与其它交换机相连的端口。

点对点链路：是两台交换机之间直接连接的链路。

➢ **MSTP**

MSTP（Multiple Spanning Tree Protocol，多生成树协议）是在 STP 和 RSTP 的基础上，根据 IEEE 协会制定的 802.1S 标准建立的，它既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。

MSTP 的特点如下：

- MSTP 通过 VLAN-实例映射表，把 VLAN 和生成树联系起来，将多个 VLAN 捆绑到一个实例中，并以实例为基础实现负载均衡。
- MSTP 把一个生成树网络划分成多个域，每个域内形成多棵内部生成树，各个生成树之间彼此独立。

- MSTP 在数据转发过程中实现 VLAN 数据的负载分担。
- MSTP 兼容 STP 和 RSTP。

➢ **MSTP 的基本概念**

MST 域（Multiple Spanning Tree Region，多生成树域）：由具有相同域配置和相同 Vlan-实例映射关系的交换机所构成。

IST（Internal Spanning Tree，内部生成树）：MST 域内的一棵生成树。

CST（Common Spanning Tree，公共生成树）：连接网络内所有 MST 域的单生成树。

CIST（Common and Internal Spanning Tree，公共和内部生成树）：连接网络内所有设备的单生成树，由 IST 和 CST 共同构成。

MSTP基本概念的组网图如图 7-2所示。

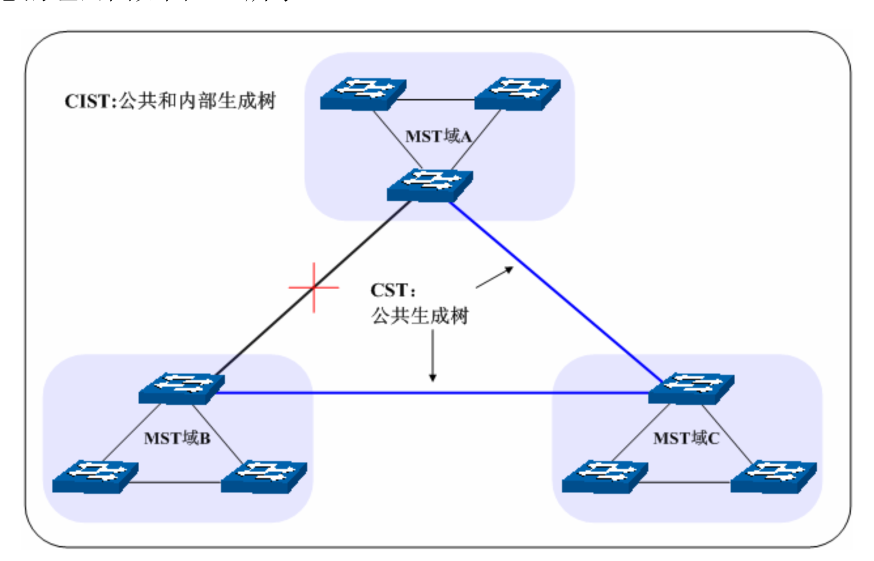


图 7-2 MSTP 基本概念组网图

➢ **MSTP 的基本原理**

MSTP 将整个网络划分为多个 MST 域，各个域之间通过计算生成 CST；域内则通过计算生成多棵生成树，每棵生成树都被称为是一个多生成树实例。MSTP 同 STP 一样，使用 BPDU 进行生成树的计算，只是 BPDU 中携带的是 MSTP 的配置信息。

➢ **MSTP 模式的 BPDU 优先级比较原则**

假定有两条 MSTP 的 BPDU X 和 Y，则：

如果 X 的总根 ID 小于 Y 的总根 ID，则 X 优于 Y

如果 X 和 Y 的总根 ID 相同，但 X 的外部路径开销小于 Y，则 X 优于 Y

如果 X 和 Y 的总根 ID 和外部路径开销相同，但 X 的域根 ID 小于 Y 的域根 ID，则 X 优于 Y

如果 X 和 Y 的总根 ID、外部路径开销和域根 ID 相同，但 X 的内部路径开销小于 Y，则 X 优于 Y

如果 X 和 Y 的总根 ID、外部路径开销、域根 ID 和内部路径开销相同，但 X 的桥 ID 小于 Y，则 X 优于 Y

如果 X 和 Y 的总根 ID、外部路径开销、域根 ID、内部路径开销和桥 ID 均相同，但 X 的端口 ID 小于 Y，则 X 优于 Y

➢ 端口状态

MSTP 中，根据端口是否转发数据和如何处理 BPDU 报文，可将端口状态划分为以下四种：

- 转发：接收并转发数据，接收并发送 BPDU 报文，进行地址学习。
- 学习：不接收或转发数据，接收并发送 BPDU 报文，进行地址学习。
- 阻塞：不接收或转发数据，接收但不发送 BPDU 报文，不进行地址学习。
- 断开：物理链路断开。

➢ 端口角色

MSTP 的端口角色分为以下几种：

- 根端口：到根桥的路径开销最低，负责向根桥方向转发数据的端口。
- 指定端口：负责向下游网段或设备转发数据的端口。
- Master 端口：连接 MST 域到总根的端口，位于整个域到总根的最短路径上。
- 替换端口：根端口和 Master 端口的备份端口。
- 备份端口：指定端口的备份端口。
- 禁用端口：物理链路断开的端口。

端口角色的示意图如图 7-3所示。

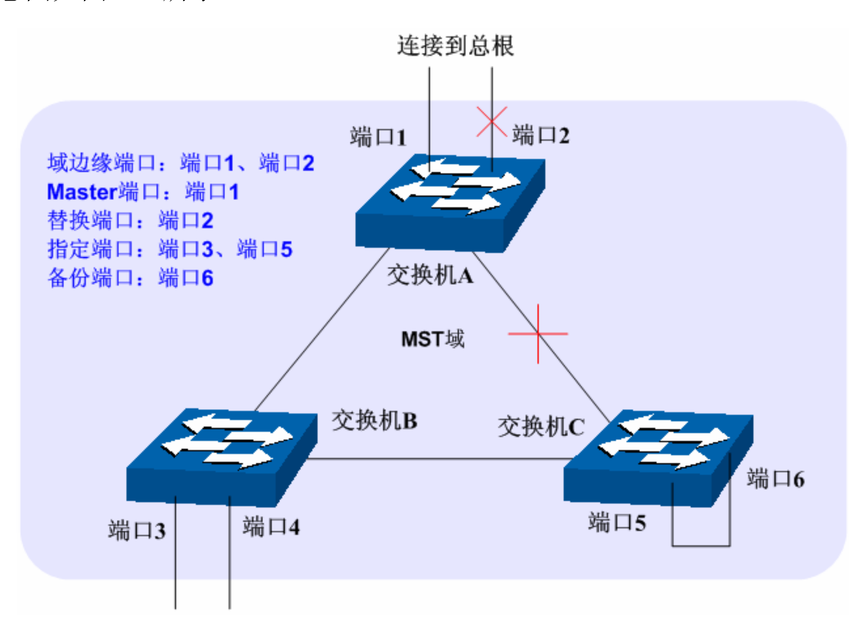


图 7-3 端口角色示意图

生成树模块主要用于配置交换机的生成树功能，包括**基本配置**、**端口配置**、**MSTP 实例**以及**安全配置**四个部分。

7.1 基本配置

基本配置用于配置和查看交换机生成树功能的全局属性，本功能包括**基本配置**和**生成树信息**两个配置页面。

7.1.1 基本配置

配置生成树前您需要明确各交换机在每个生成树实例中所处的地位，每个生成树实例中只有一台交换机处于根桥地位。配置交换机的生成树功能，首先需要在本页配置交换机生成树的全局功能和相关参数。

进入页面的方法：生成树>>基本配置>>基本配置

全局配置

生成树功能： ○ 启用 ◉ 禁用

生成树模式： STP

提交

参数配置

CIST优先级： 32768 （0 - 61440，4096为间隔）

联络时间： 2 秒（1-10）

老化时间： 20 秒（6-40）

传输时延： 15 秒（4-30）

流量限制： 5 pps（1-20）

最大跳数： 20 跳（1-40）

提交

帮助

图 7-4 基本配置

条目介绍：

➢ 全局配置

生成树功能： 选择是否启用交换机的生成树功能。

生成树模式： 选择交换机的生成树模式。

- STP：生成树兼容模式。
- RSTP：快速生成树兼容模式。
- MSTP：多重生成树模式。

➢ 参数配置

CIST 优先级： 填写交换机的 CIST 优先级。CIST 优先级是确定交换机是否会被选为根桥的重要依据，同等条件下优先级高的交换机将被选为根桥。值越小，表示优先级越高。默认为 32768，且必须是 4096 的倍数。

联络时间： 填写交换机发送协议报文的周期，用于检测链路是否存在故障。并且，2×(联络时间+1)≤老化时间。默认为 2 秒。

老化时间： 填写协议报文在交换机中能够保存的最大生存期。默认为 20 秒。

传输时延： 在网络拓扑改变后，交换机的端口状态迁移的延时时间。并且，2×(传输延时－1)≥老化时间。默认为 15 秒。

流量限制： 填写在每个联络时间内，端口最多能够发送的协议报文的速度。默认为 5pps。

最大跳数： 填写协议报文被转发的最大跳数，限制生成树的规模，默认 20 跳。

注意：

- 设备的传输时延参数的长短与 STP 的规模有关。如果传输时延过小，可能会引入临时的环路；如果传输时延过大，网络可能会较长时间不能恢复连通，建议采用默认值。
- 合适的联络时间可以保证设备能够及时发现网络中的链路故障，又不会占用过多的网络资源。如果联络时间过长，在链路发生丢包时，交换机会误以为链路出现了故障，从而引发网络中生成树的重新计算；如果联络时间过短，交换机将频繁发送重复的配置消息，增加了交换机的负担，浪费了网络资源，建议采用默认值。
- 如果老化时间过小，交换机会频繁地计算生成树，而且有可能将网络拥塞误认成链路故障；如果老化时间过大，交换机不能及时发现链路故障，不能及时重新计算生成树，从而降低网络的自适应能力，建议采用默认值。
- 如果流量限制过大，每个联络时间内发送的 MSTP 报文数会很多，从而占用过多的网络资源，建议采用默认值。

7.1.2 生成树信息

本页用来查看交换机生成树功能的相关参数。

进入页面的方法：生成树>>基本配置>>生成树信息

生成树信息	
开启状态：	启用
STP版本：	MSTP
本桥：	32768---00-02-03-c0-9a-d3
总根：	32768---00-02-03-c0-9a-d3
外部路径开销：	0
域根：	32768---00-02-03-c0-9a-d3
内部路径开销：	0
指定桥：	32768---00-02-03-c0-9a-d3
根端口：	---
上次拓扑改变时间：	2006-01-01 10:43:30
拓扑改变次数：	1

MSTP实例信息	
实例ID：	1
开启状态：	启用
本桥：	32768---00-02-03-c0-9a-d3
域根：	32768---00-02-03-c0-9a-d3
内部路径开销：	0
指定桥：	32768---00-02-03-c0-9a-d3
根端口：	---
上次拓扑改变时间：	2006-01-01 10:44:41
拓扑改变次数：	1

刷新

图 7-5 基本信息

7.2 端口配置

本页用来配置交换机端口的 CIST 参数。

进入页面的方法：生成树>>端口配置



端口配置

端口 [ ] 选择

选择	端口	状态	优先级	外部路径开销	内部路径开销	边缘端口	点对点链路	协议迁移	工作模式	端口角色	端口状态	LAG
		禁用				禁用	自动	不改变				
	1	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
	2	启用	128	19(自动)	19(自动)	禁用	开启(自动)	---	STP	指定端口	转发	---
	3	启用	128	100(自动)	100(自动)	禁用	关闭(自动)	---	---	禁用端口	断开	---
	4	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
	5	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
	6	启用	128	100(自动)	100(自动)	禁用	关闭(自动)	---	---	禁用端口	断开	---
	7	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
	8	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
	9	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
	10	启用	128	19(自动)	19(自动)	禁用	开启(自动)	---	STP	指定端口	转发	---
	11	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
	12	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
	13	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
	14	禁用	128	自动	自动	禁用	自动	---	---	---	---	---
	15	禁用	128	自动	自动	禁用	自动	---	---	---	---	---

提交 刷新 帮助

注意：
将路径开销设置为0，即可根据端口连接速率自动设置路径开销。

图 7-6 端口配置

条目介绍：

➢ 端口配置

端口选择：	点击<选择>按键，可根据所输端口号，快速选择相应端口。
选择：	勾选端口配置端口 STP 功能，可多选。
端口：	显示交换机的端口号。
状态：	选择该端口是否启用 STP 功能。
优先级：	确定与该端口连接的端口是否会被选为根端口的重要依据。同等条件下优先级高的端口将被选为根端口。值越小，表示优先级越高。默认为 128，范围 0-240，且为 16 的倍数。
外部路径开销：	在不同 MST 域之间的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高。
内部路径开销：	在 MST 域内的路径上，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高。
边缘端口：	选择是否启用边缘端口。边缘端口由阻塞状态向转发状态迁移时，可实现快速迁移，无需等待延迟时间。

点对点链路： 选择端口的点对点链路状态。以点对点链路相连的两个端口，如果为根端口或者指定端口，则可以快速迁移到转发状态，从而减少不必要的转发延迟时间。

协议迁移： 启用端口开始一次协议迁移检查。

工作模式： 显示端口所处的生成树模式。

端口角色： 显示端口在生成树实例中担任的角色。

- 根端口：到根桥的路径开销最低，负责向根桥方向转发数据的端口。
- 指定端口：负责向下游网段或设备转发数据的端口。
- Master 端口：连接多生成树域到总根的端口，位于整个域到总根的最短路径上。
- 替换端口：根端口和 Master 端口的备份端口。
- 备份端口：指定端口的备份端口。
- 禁用端口：物理链路断开的端口。

端口状态： 显示端口所处的工作状态。

- 转发：接收并转发数据，接收并发送协议报文，进行地址学习。
- 学习：不接收或转发数据，接收并发送协议报文，进行地址学习。
- 阻塞：不接收或转发数据，接收但不发送协议报文，不进行地址学习。
- 断开：物理链路断开。

LAG： 显示端口当前所属的汇聚组。

注意：

- 对于直接与终端相连的端口，请将该端口设置为边缘端口，同时启动 BPDU 保护功能。这样既能够使该端口快速迁移到转发状态，也可以保证网络的安全。
- 对于属于汇聚组的端口，所有端口都可以被配置成与点对点链路相连。
- 当端口被设置为与点对点链路相连，则该端口所在的所有生成树实例均被设置为与点对点链路相连。如果端口实际物理链路不是点对点链路，而您配置为强制点对点链路，则有可能会引入临时环路。

7.3 MSTP实例

MSTP 设置了 VLAN-实例映射表（即 VLAN 和生成树的对应关系表），把 VLAN 和生成树联系起来。通过增加 MSTP 实例（将多个 VLAN 整合到一个集合中），将多个 VLAN 捆绑到一个实例中，并以实例为基础实现负载均衡。

只有当多台交换机的 MST 域名、MST 域的修订级别、VLAN-实例映射表完全相同时，它们才能属于同一个 MST 域。本功能包括**域配置**、**实例配置**和**实例端口**三个配置页面。

7.3.1 域配置

本页用来配置 MST 域的域名和修订级别。

进入页面的方法：生成树>>**MSTP** 实例>>域配置

域配置

域名：00-02-03-c0-9a-d3

修订级别：0 （0 - 65535）

提交 帮助

图 7-7 域配置

条目介绍：

➢ 域配置

域名：填写域名来标识 MST 域，最长可用 32 个字符。

修订级别：填写修订级别来标识 MST 域。

7.3.2 实例配置

实例配置是 MST 域的一个属性，用来描述 VLAN 和生成树实例的映射关系。您可以按需要将 VLAN 分配至不同的实例，每个实例就是一个“VLAN 组”，不受其它实例和公共生成树的影响。

进入页面的方法：生成树>>**MSTP** 实例>>实例配置

实例配置

实例ID [ ] 选择

选择	实例ID	状态	优先级	VLAN ID	
☐		禁用			
☐	1	禁用	32768		删除映射
☐	2	禁用	32768		删除映射
☐	3	禁用	32768		删除映射
☐	4	禁用	32768		删除映射
☐	5	禁用	32768		删除映射
☐	6	禁用	32768		删除映射
☐	7	禁用	32768		删除映射
☐	8	禁用	32768		删除映射
	CIST	启用	32768	1-4094,	

提交 帮助

VLAN-实例映射

VLAN ID： （1 - 4094）

实例ID： （0 - 8，0代表CIST）

提交

注意：

1、VLAN ID输入格式例如：'1,3,4-7,9,11-30'，且VID范围取1-4094

图 7-8 实例配置

条目介绍：

➢ 实例配置

实例 ID 选择： 点击<选择>按键，可根据所输 ID 号，快速选择相应实例。

选择： 勾选条目配置实例状态及优先级，可多选。

实例 ID： 显示交换机的实例 ID 号。

状态： 选择是否启用相应实例。

优先级： 在对应实例 ID 中，确定该交换机是否会被选为根桥的重要依据。默认为 32768，且必须是 4096 的倍数。

VLAN ID： 填写该实例 ID 所包含的 VLAN ID。若之前已存在 VLAN ID，在此修改后，之前的 VLAN ID 将被清空，并映射至 CIST 中。

➢ **VLAN-实例映射**

VLAN ID： 填写需要添加的 VLAN ID。若对应实例 ID 中已有 VLAN ID，在此修改后，新的 VLAN ID 将被添加，而不会将之前的覆盖。

实例 ID： 填写实例 ID。



注意：

- 当GVRP和MSTP同时启用时，GVRP报文将沿着生成树实例CIST进行传播。因此如果希望通过GVRP在网络中发布某个VLAN，则需在配置MSTP的"VLAN-实例映射"时保证把这个VLAN映射到CIST上。关于GVRP的相关介绍请参见6.4 GVRP。

7.3.3 实例端口

端口在不同的生成树实例中可以担任不同的角色，本页用来配置不同实例 ID 中的端口的参数，同时在此可以查看端口在特定实例中的状态信息。

进入页面的方法：生成树>>MSTP 实例>>实例端口



图 7-9 实例端口

条目介绍：

➢ 实例端口配置

实例 ID： 选择需要配置端口属性的实例 ID。

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

选择： 勾选端口配置端口的优先级和路径开销，可多选。

端口： 显示交换机的端口号。

优先级： 在对应实例 ID 中，确定与该端口连接的端口是否会被选为根端口的重要依据。默认为 128，范围 0-240，且为 16 的倍数。

路径开销： 在 MST 域内的对应实例中，用于选择路径和计算路径开销的参考值，同时也是确定该端口是否会被选为根端口的依据。值越小，表示优先级越高。

端口角色： 显示端口在生成树实例中担任的角色。

端口状态： 显示端口所处的工作状态。

LAG： 显示端口当前所属的汇聚组。

注意：

- 同一端口在不同的生成树实例中的端口状态可以不同。

安全树功能全局配置步骤：

步骤	操作	说明
1	明确交换机在生成树实例中的角色：根桥或指定桥	准备工作。
2	配置 MSTP 的全局参数	必选操作。在**生成树>>基本配置>>基本配置**页面，开启交换机的生成树功能，并配置 MSTP 的参数。
3	配置端口的 MSTP 参数	必选操作。**生成树>>端口配置>>端口配置**页面进行配置。
4	配置 MST 域	必选操作。**生成树>>MSTP 实例>>域配置**、**实例配置**页面，创建 MST 域，及交换机在 MST 域中的角色。
5	配置实例端口的 MSTP 参数	可选操作。**生成树>>MSTP 实例>>实例端口**页面，为 MST 域内不同的实例，配置实例端口的 MSTP 属性。

7.4 安全配置

通过配置设备的保护功能，来防止生成树网络中的设备遭受各种形式的恶意攻击。本功能包括**端口保护**和 **TC 保护**两个配置页面。

7.4.1 端口保护

➢ **环路保护：**

在网络拓扑稳定时，交换机通过不断接收上游交换机发送的 BPDU 报文，来保持本机各个端口的端口状态。但是当发生链路拥塞或者单向链路故障时，位于下游的交换机无法收到 BPDU 报文，将会重新计算生成树，重新选择端口角色，这时阻塞端口会迁移到转发状态，从而导致网络中产生环路。

环路保护功能会抑制这种环路的产生。对于启用了环路保护的端口，当没有接收到上游交换机发送的 BPDU 报文，引起 STP 重新计算时，不论其端口角色如何，该端口将一直被设置为阻塞状态。

➢ **根桥保护：**

在设计网络拓扑时，CIST 的根桥和备份根桥大多处于一个高带宽的核心域内。但是，当维护人员错误配置或遭受到网络中的恶意攻击时，网络中的合法根桥有可能会收到优先级更高的 BPDU 报文，致使当前合法根桥失去了根桥的地位，从而导致网络拓扑结构的错误变动。这种错误的变动，使得原来应该通过高速链路的流量被牵引到低速链路上，引起网络拥塞。

为了防止这种情况发生，MSTP 提供根桥保护功能：对于启用了根桥保护功能的端口，它在所有实例上的端口角色只能为“指定端口”。当该端口收到优先级更高的 BPDU 时，立刻将该端口的端口状态转化为“阻塞”状态，不再转发报文（相当于将此端口相连的链路断开）。当在 2 倍的传输时延时间内没有收到更优的配置消息时，端口会恢复原来的正常状态。

➢ **TC 保护**

交换机收到 TC-BPDU 报文（网络拓扑发生变化的通知报文）后，会将本机的地址表项删除。当有人伪造 TC-BPDU 报文恶意攻击交换机时，交换机短时间内收到大量 TC-BPDU 报文，频繁的删除操作给交换机带来很大负担，给网络的稳定带来很大隐患。通过在交换机上启用 TC 保护功能，可以避免交换机频繁地删除地址表项。

启用 TC 保护功能后，交换机在“TC 保护周期”内，收到 TC-BPDU 的最大数目为“TC 保护阈值”

处所设的数目，超过该数目后，交换机在该周期内不再进行地址表删除操作。这样就可以避免频繁地删除转发地址表项。

➢ **BPDU 保护**

交换机上直接与 PC 或服务器相连的端口会被设置为“边缘端口”，以实现这些端口的快速迁移。当这些端口接收到 BPDU 报文时系统会自动将这些端口设置为非边缘端口，重新计算生成树，引起网络拓扑结构的变化。而这些端口一般情况下不会收到 BPDU 报文。如果有人用伪造的 BPDU 报文恶意攻击交换机，就会引起网络拓扑的震荡。

MSTP 提供 BPDU 保护功能来防止这种攻击：启用了 BPDU 保护功能后，如果边缘端口收到了 BPDU 报文，MSTP 就将这些端口关闭，同时通知网管这些端口被 MSTP 关闭，被关闭的端口只能由网络管理人员来恢复。

➢ **BPDU 过滤**

BPDU 过滤用来防止恶意的 BPDU 洪泛攻击。交换机收到恶意的 BPDU 报文以后，会向网络中的其它交换机转发，致使网络内的交换机不停的进行 STP 计算，从而导致交换机的 CPU 占用率过高或者 BPDU 报文的协议状态错误等。

启用了 BPDU 报文过滤功能的端口，将不再接收和转发任何 BPDU 报文，但是会向外发送自身的 BPDU 报文，从而防止交换机受到 BPDU 报文的攻击，保证 STP 计算的正确性。

在本页可以对交换机的各个端口配置上述几种保护功能，建议您对符合条件的端口启用相应的保护功能。

进入页面的方法：生成树>>安全配置>>端口保护

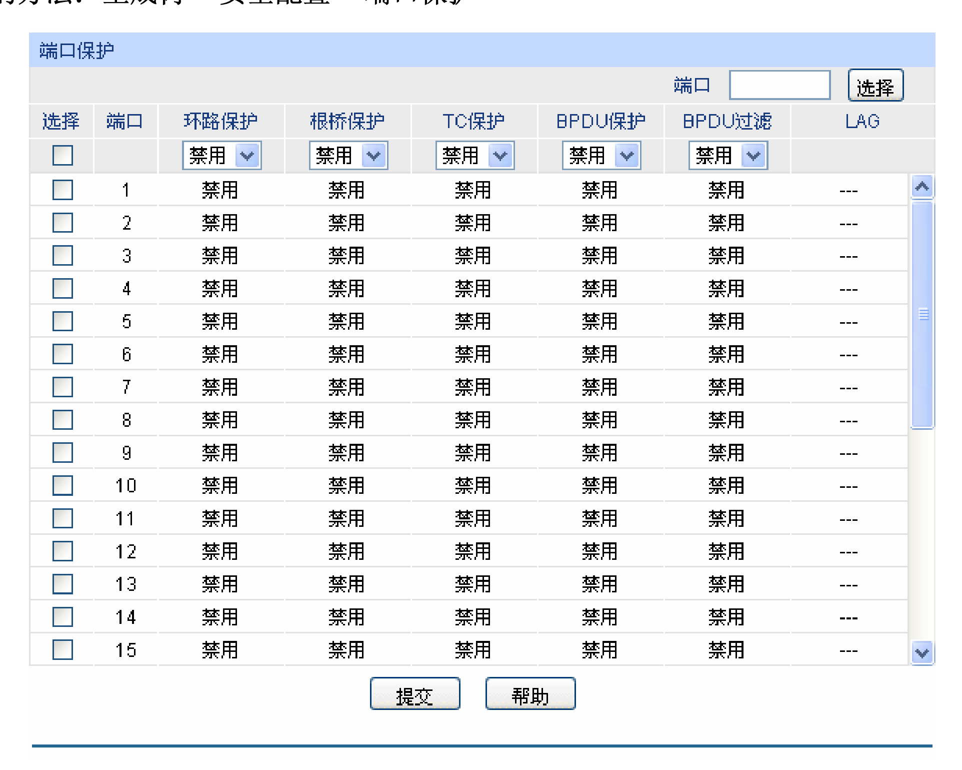


图 7-10 端口保护

条目介绍：

➢ 端口保护

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

选择： 勾选端口配置端口保护功能，可多选。

端口： 显示交换机的端口号。

环路保护： 防止由于链路拥塞或者单向链路故障，导致下游设备重新计算生成树，由此产生的网络环路现象。

根桥保护： 防止当前合法根桥失去根桥的地位而引起网络拓扑结构的错误变动。

TC 保护： 防止由于恶意伪造的 TC 报文在 STP 协议网络中传播而导致桥设备的地址表不断清空所引起的网络吞吐量下降。

BPDU 保护： 防止边缘端口受到恶意伪造的协议报文的攻击。

BPDU 过滤： 防止 STP 协议网络中协议报文泛洪。

LAG： 显示端口当前所属的汇聚组。

7.4.2 TC保护

当**端口保护**页面开启端口的“TC 保护”功能后，需要在本页对 TC 保护的 TC 保护阈值和 TC 保护周期进行配置。

进入页面的方法：**生成树>>安全配置>>TC 保护**

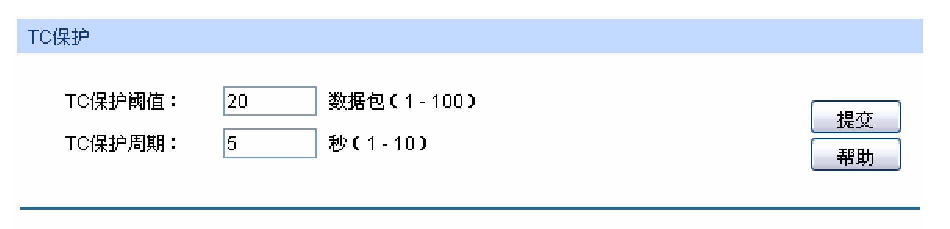


图 7-11 TC 保护

条目介绍：

> **TC 保护**

TC 保护阈值： 在 TC 保护周期内，交换机收到 TC 报文的最大数目。超过该数目后，交换机在该周期内不再进行地址表删除操作。默认为 20 数据包。

TC 保护周期： 填写 TC 保护的周期。默认为 5 秒。

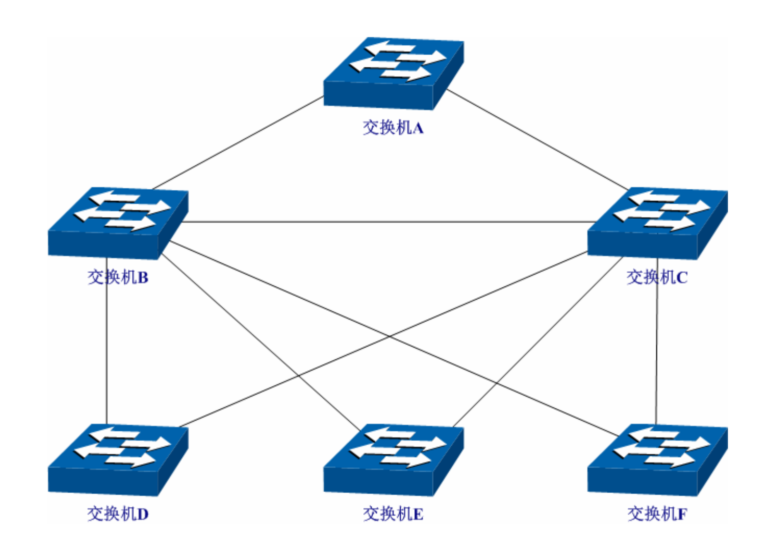
7.5 STP功能的组网应用

> 组网需求

- 交换机 A、B、C、D、E 均支持 MSTP 功能；
- A 为中心交换机；
- B、C 为汇聚层交换机，D、E、F 为接入层交换机；
- 整个网络中共有 6 个 VLAN，为 VLAN101-VLAN106；

- 所有设备运行 MSTP，并且所有设备均属于同一个 MST 域；
- VLAN101、103 和 105 的数据流量以 B 为根桥，VLAN102、104 和 106 的数据流量以 C 为根桥。阻断网络中的环路，并能达到数据转发过程中 VLAN 数据的冗余备份以及负载分担效果。

➢ **组网图**



➢ **配置步骤**

- 配置交换机 A：

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为Trunk，并将端口加入VLAN 101 到VLAN 106。具体配置方法请参见6.1 802.1Q VLAN。
2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择 MSTP 生成树模式。 在**生成树>>基本配置>>端口配置**页面，启用端口的 MSTP 功能。
3	配置 MST 域的域名和修订级别	在**生成树>>MSTP 实例>>域配置**页面，配置域名为“TP-LINK”，修订级别默认即可。
4	配置 MST 域的 VLAN-实例映射	在**生成树>>MSTP 实例>>实例配置**页面，配置 VLAN-实例映射表。将 VLAN101、103 和 105 映射到实例 1，将 VLAN102、104 和 106 映射到实例 2。

- 配置交换机 B：

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为Trunk，并将端口加入VLAN 101 到VLAN 106。具体配置方法请参见6.1 802.1Q VLAN。

2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择 MSTP 生成树模式。 在**生成树>>基本配置>>端口配置**页面，启用端口的 MSTP 功能。
3	配置 MST 域的域名和修订级别	在**生成树>>MSTP 实例>>域配置**页面，配置域名为“TP-LINK”，修订级别默认即可。
4	配置 MST 域的 VLAN-实例映射	在**生成树>>MSTP 实例>>实例配置**页面，配置 VLAN-实例映射表。将 VLAN101、103 和 105 映射到实例 1，将 VLAN102、104 和 106 映射到实例 2。
5	将交换机 B 配置为实例 1 的根桥	在**生成树>>MSTP 实例>>实例配置**页面，将实例 1 的优先级设置为 0
6	将交换机 B 配置为实例 2 的指定桥	在**生成树>>MSTP 实例>>实例配置**页面，将实例 2 优先级设置为 4096

● 配置交换机 C

步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为Trunk，并将端口加入VLAN 101 到VLAN 106。具体配置方法请参见6.1 802.1Q VLAN。
2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择 MSTP 生成树模式。 在**生成树>>基本配置>>端口配置**页面，启用端口的 MSTP 功能。
3	配置 MST 域的域名和修订级别	在**生成树>>MSTP 实例>>域配置**页面，配置域名为“TP-LINK”，修订级别默认即可。
4	配置 MST 域的 VLAN-实例映射	在**生成树>>MSTP 实例>>实例配置**页面，配置 VLAN-实例映射表。将 VLAN101、103 和 105 映射到实例 1，将 VLAN102、104 和 106 映射到实例 2。
5	将交换机 C 配置为实例 1 的指定桥	在**生成树>>MSTP 实例>>实例配置**页面，将实例 1 的优先级设置为 4096。
6	将交换机 C 配置为实例 2 的根桥	在**生成树>>MSTP 实例>>实例配置**页面，将实例 2 优先级设置为 0。

● 配置交换机 D

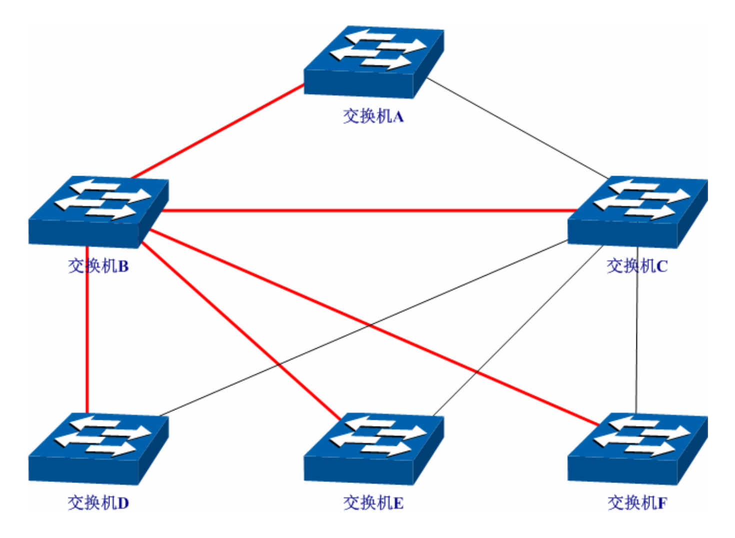
步骤	操作	说明
1	配置端口	在“802.1Q VLAN”功能处，相应端口的类型为Trunk，并将端口加入VLAN 101 到VLAN 106。具体配置方法请参见6.1 802.1Q VLAN。

2	启用生成树功能。	在**生成树>>基本配置>>基本配置**页面，启用生成树功能，选择 MSTP 生成树模式。 在**生成树>>基本配置>>端口配置**页面，启用端口的 MSTP 功能。
3	配置 MST 域的域名和修订级别	在**生成树>>MSTP 实例>>域配置**页面，配置域名为“TP-LINK”，修订级别默认即可。
4	配置 MST 域的 VLAN-实例映射	在**生成树>>MSTP 实例>>实例配置**页面，配置 VLAN-实例映射表。将 VLAN101、103 和 105 映射到实例 1，将 VLAN102、104 和 106 映射到实例 2。

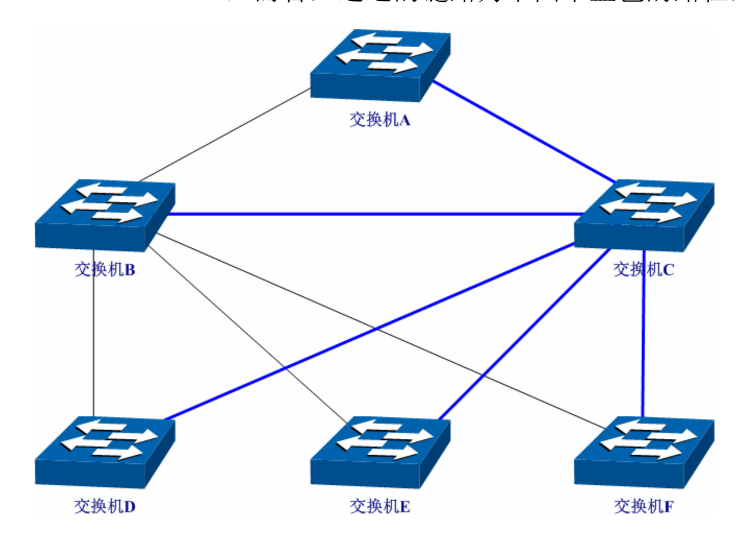
- 交换机 E 和交换机 F 的配置方法同交换机 D

➢ **拓扑稳定以后两个实例所生成的动态拓扑结构**

- 对于实例 1（VLAN 101 103 105）而言，连通的链路为下图中红色的路径，灰色的路径断开。



- 对于实例 2（VLAN 102 104 106）而言，连通的链路为下图中蓝色的路径，灰色的路径断开。



➢ **配置建议**

- 所有交换机的端口均建议启用“TC 保护”功能。
- 根桥交换机的所有端口建议启用“根桥保护”功能。

- 非边缘端口建议启用“环路保护”功能。
- 连接 PC 与服务器的边缘端口，建议启用“BPDU 保护”或“BPDU 过滤”功能。

回目录

第8章 组播管理

➢ 组播概述

在网络中，存在着三种发送报文的方式：单播、广播、组播。数据采用单播（Unicast）方式传输时，服务器会为每一个接收者单独传输一份信息，如果有多个接收者存在，网络上就会重复地传输多份相同内容的信息，这样将会大量占用网络资源。数据采用广播（Broadcast）方式传输时，系统会把信息一次性的传送给网络中的所有用户，不管他们是否需要，任何用户都会接收到广播来的信息。

当前，诸如视频会议和视频点播等单点发送、多点接收的多媒体业务正在成为信息传送的重要组成部分。在一点发送多点接收的前提下，单播方式适合用户较少的网络，而广播方式适合用户稠密的网络，当网络中需求某信息的用户量不确定时，单播和广播方式效率很低。这时组播（multicast）应运而生，它实现了网络中单点到多点的高效数据传送，能够节约大量网络带宽，降低网络负载。组播传输信息的方式如图 8-1所示。

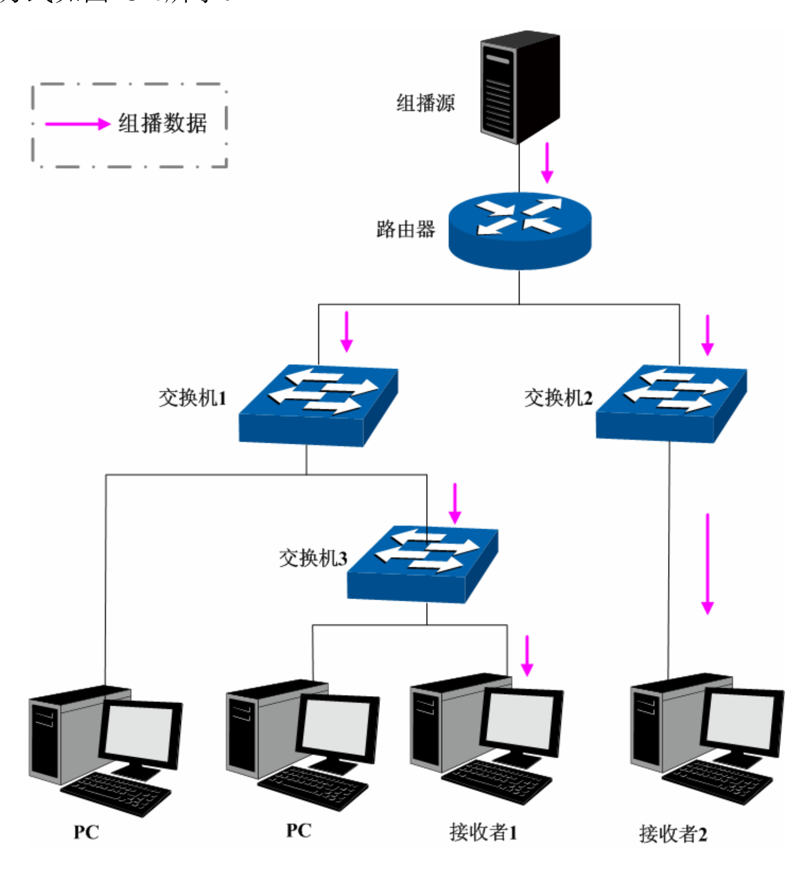


图 8-1 组播传输信息的方式

组播的特点是：

- 服务对象不固定，通常是一对多的关系；
- 把服务对象看成一个组，发送端只需要发送一次数据到相关网络设备即可；
- 每个用户可以随时加入或退出组播组；
- 实时性要求较高，允许一定的丢帧现象发生。

➢ 组播地址

组播 IP 地址：

根据 IANA（Internet Assigned Numbers Authority，因特网编号授权委员会）规定，组播报文的 IP 地址使用 D 类 IP 地址，组播 IP 地址范围是 224.0.0.0～239.255.255.255。其中，几个特殊组播 IP 地址段的范围及说明如下：

组播地址范围	说明
224.0.0.0～224.0.0.255	路由协议及其它底层拓扑发现和维护协议的保留地址
224.0.1.0～224.0.1.255	会议及电视会议
239.0.0.0～239.255.255.255	局域网内部使用地址，不能用于 internet

表 8-1 特殊的组播 IP 地址段

组播 MAC 地址：

以太网传输单播 IP 报文的时候，目的 MAC 地址使用的是接收者的 MAC 地址。但是在传输组播报文时，传输目标不再是一个具体的接收者，而是一个成员不确定的组，所以需要使用组播 MAC 地址作为目的地址，组播 MAC 地址是一个逻辑的 MAC 地址。

IANA规定，组播MAC地址的高 24bit位是以 01-00-5E开头，低 23bit为组播IP地址的低 23bit，映射关系如图 8-2所示：

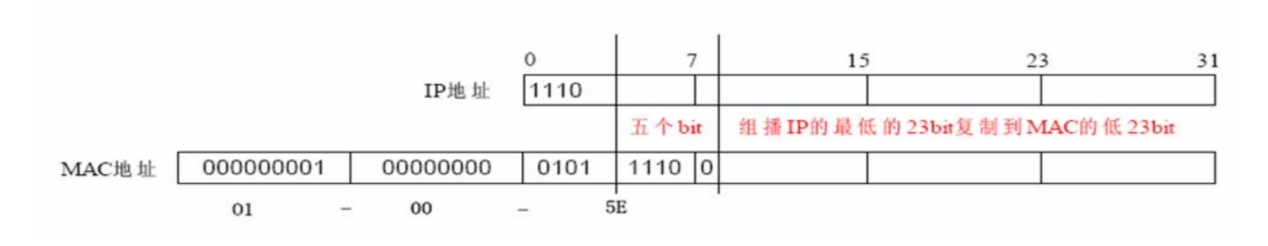


图 8-2 组播 MAC 地址和组播 IP 地址的对应关系

由于 IP 组播地址的高 4bit 是 1110，标识了组播组，而低 28bit 中只有 23bit 被映射到组播 MAC 地址上，这样 IP 组播地址中就会有 5bit 没有使用，从而出现了 32 个 IP 组播地址映射到同一 MAC 地址上的结果。

- **组播地址表**

交换机在转发组播数据时是根据组播地址表来进行的。由于组播数据不能跨越VLAN传输，因此组播地址表的第一部分是VLAN ID，当交换机收到组播数据包时，数据包只能在接收端口所在的VLAN内转发。组播地址表对应的出口端口不是一个，而是一组端口列表。转发数据时，交换机根据组播数据的目的组播地址查找组播地址表，如果在组播地址表中查不到相应的条目，则把该组播数据广播，即向接收端口所在VLAN内的所有端口上转发；如果能查找到对应的条目，则目的地址应该是一组端口列表，于是交换机把这个组播数据复制成多份，每份转发到一个端口，从而完成组播数据的交换。组播地址表一般格式如图 8-3所示。

VLAN ID	组播 IP	端口

图 8-3 组播地址表

- **IGMP 侦听**

网络中的主机通过发送 IGMP（Internet Group Management Protocol，互联网组管理协议）报文向临近的路由器申请加入（或离开）组播组，当上层路由设备将组播数据转发下来后，交换机负责将组播数据转发给主机。IGMP 侦听（IGMP Snooping）是组播约束机制，交换机用他来完成组播组

的动态注册，运行 IGMP 侦听的交换机通过侦听和分析主机与组播路由器之间交互的 IGMP 报文来管理和控制组播组，从而可以有效抑制组播数据在网络中扩散。

组播管理模块主要用于配置交换机的组播管理功能，包括 **IGMP 侦听**、**组播地址表**、**组播过滤**以及**报文统计**四个部分。

8.1 IGMP侦听

- **IGMP 侦听的工作过程**

交换机侦听用户主机与路由器之间的交互 IGMP 报文，跟踪组播信息及其申请的端口。当交换机侦听到主机向路由器发出报告报文（IGMP Report）时，交换机便把该端口加入组播地址表中；当交换机侦听到主机发送的离开报文（IGMP Leave）时，路由器会发送该端口的特定组查询报文（Group-Specific Query），若还有其它主机需要该组播，则将回应报告报文，若路由器收不到任何主机的回应，交换机便把该端口从组播地址表中删除。路由器会定时发查询报文（IGMP Query），交换机收到查询报文后，如果在一定的时间段内没有收到主机的报告报文，便把该端口从组播表中删除。

- **IGMP 报文**

运行了 IGMP 侦听的交换机对不同类型的 IGMP 报文的处理方法如下。

1. 查询报文（IGMP Query）。

由路由器发出，又可分为通用查询报文和特定组查询报文。路由器定时发出通用查询报文，以查询该网段有哪些组播组的成员。当路由器收到 IGMP 离开报文后，会通过接收端口向该组播组发送 IGMP 特定组查询报文，交换机会将此报文转发，以确定该端口中是否还有组播组的其它组成员。

对于通用查询报文，交换机会将此报文通过 VLAN 内除接收端口以外的其它端口转发，并对接收端口做出相应的处理：如果接收端口不是已有路由器端口，则将其加入路由器端口列表，并启用路由器端口时间；如果是已有路由器端口，则直接重置路由器端口时间。

对于特定组查询报文，交换机要向被查询的组播组的成员转发 IGMP 特定组查询报文。

2. 报告报文（IGMP Report）。

由主机发出，当主机想主动加入某一组播组或对路由器查询报文给予响应时产生此种报文。

在收到 IGMP 报告报文时，交换机将此报文通过 VLAN 内的路由器端口转发出去，同时从该报文中解析出主机要加入的组播组地址，并对该报文的接收端口做相应的处理：如果接收端口是新成员端口，则将其加入到组播地址表中，并启用该端口的成员端口时间；如果接收端口是旧成员端口，则直接重置成员端口时间。

3. 离开报文（IGMP Leave）。

运行 IGMPv1 的主机离开组播组时不会发送 IGMP 离开报文，因此交换机无法立即获知主机离开的信息。但是，由于主机离开组播组后不会再发送 IGMP 报告报文，因此当其对应的成员端口时间超时后，交换机就会将该端口从相应的组播地址表中删除。运行 IGMPv2 或 IGMPv3 的主机离开组播组时，会通过发送 IGMP 离开报文，以通知组播路由器自己离开了某个组播组。

当交换机从某一端口收到 IGMP 离开报文时，为了确认此端口下是否还有其它组成员存在，交换机向此端口转发特定组查询报文，然后重置成员端口时间为离开滞后时间，离开滞后时间超时后，交换机将此端口从相应的组播地址表中删除。如果删除离开端口后组播组中没有其它组成员存在，则将整个组播组删除。

➢ **IGMP 侦听的基本概念**

1. 相关端口

路由器端口（Router Port）：交换机上连接路由组播设备的端口。

成员端口（Member Port）：交换机上连接组播组成员的端口。

2. 相关定时器

路由器端口时间：这段时间内，如果交换机没从路由器端口接收到查询报文，就认为该路由器端口失效。默认是 300 秒。

成员端口时间：这段时间内，如果交换机没接收到成员端口发送的查询报文，就认为该成员端口不再有主机属于多播组。默认是 260 秒。

离开滞后时间：从主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。默认是 1 秒。

本功能包括**基本配置**、**端口参数**、**VLAN 参数**和**组播 VLAN** 四个配置页面。

8.1.1 基本配置

配置本交换机的 IGMP 侦听功能，首先要在本页配置 IGMP 侦听的全局功能和相关参数。

如果交换机收到的组播数据没有在组播地址表内，该组播数据会在 VLAN 内广播；当交换机启用"未知组播报文丢弃"功能后，交换机收到不在组播地址表中的组播数据报文时，会将此报文丢弃，从而节省带宽，并提高系统的处理效率，请根据实际情况配置该功能。

进入页面的方法：组播管理>>IGMP 侦听>>基本配置

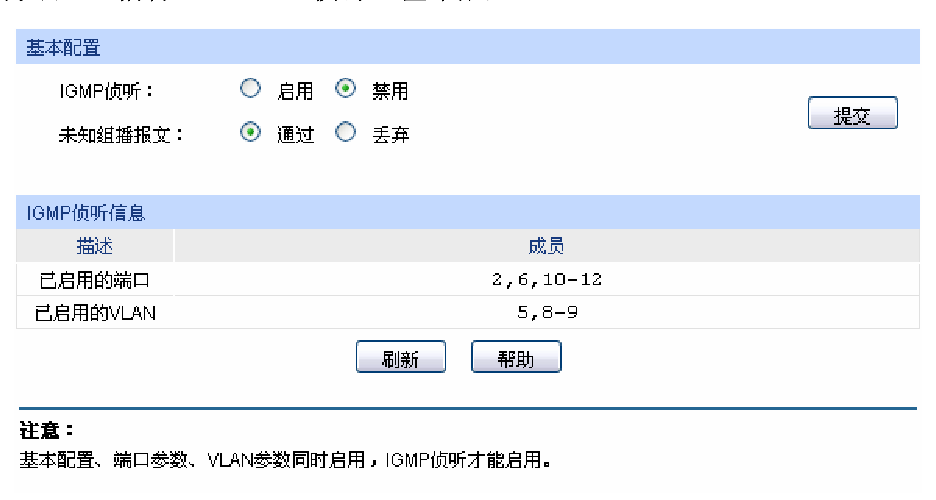


图 8-4 基本配置

条目介绍：

➢ 端口配置

IGMP 侦听：	选择是否启用交换机的 IGMP 侦听功能。
未知组播报文：	选择交换机对未知组播报文的处理方法。

➢ **IGMP 侦听信息**

描述：	显示 IGMP 侦听的配置项。

成员： 显示对应配置项的成员。

8.1.2 端口参数

本页用来配置交换机端口的 IGMP 侦听属性。

进入页面的方法：组播管理>>IGMP 侦听>>端口参数



图 8-5 端口参数

条目介绍：

- 端口配置

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

选择： 勾选条目配置端口的 IGMP 侦听功能，可多选。

端口： 显示交换机的端口号。

IGMP 侦听： 选择该端口是否启用 IGMP 侦听功能。

快速离开功能： 当端口启动快速离开功能后，交换机收到 IGMP 离开报文时，直接将该端口从组播组中删除。

LAG： 显示端口当前所属的汇聚组。

注意：

- 端口的快速离开功能只能在主机支持 IGMPv2 或 v3 时生效。
- 当快速离开功能与“未知组播报文丢弃”功能同时开启的情况下，如果某个端口下有多个用户，一个用户的快速离开，可能会造成同一组播组中其它用户的组播业务中断。

8.1.3 VLAN参数

IGMP 侦听所建立的组播组是基于 VLAN 广播域的，不同的 VLAN 可以设置不同的 IGMP 参数。本

页用于配置每个 VLAN 的 IGMP 侦听参数。

进入页面的方法：组播管理>>IGMP 侦听>>VLAN 参数

VLAN参数

VLAN ID： （1-4094）

路由器端口时间： 秒（60-600，推荐300秒）

成员端口时间： 秒（60-600，推荐260秒） 添加

离开滞后时间： 秒（1-30，推荐1秒）

静态路由端口： 禁用

VLAN列表

VLAN ID 选择

选择	VLAN ID	路由器端口时间	成员端口时间	离开滞后时间	路由器端口
☐					
☐	5	300	260	1	---
☐	8	300	260	1	---
☐	9	300	260	1	5（静态）

提交 删除 帮助

注意：

当组播VLAN功能启用时，此处配置将失效。

图 8-6 VLAN 参数

条目介绍：

- **VLAN 参数**

VLAN ID： 填写启用 IGMP 侦听功能的 VLAN ID。

路由器端口时间： 在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。推荐 300 秒。

成员端口时间： 在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。推荐 260 秒。

离开滞后时间： 主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。推荐 1 秒。

静态路由端口： 选择静态配置的路由器端口，多用于拓扑稳定的网络中。

- **VLAN 列表**

VLAN ID 选择： 点击<选择>按键，可根据所输 VLAN ID，快速查找 VLAN 条目。

选择： 勾选条目配置 VLAN 参数，可多选。

VLAN ID： 显示 VLAN ID。

路由器端口时间： 显示 VLAN 的路由器端口时间。

成员端口时间： 显示 VLAN 的成员端口时间。

离开滞后时间： 显示 VLAN 的离开滞后时间。

路由器端口： 显示 VLAN 的路由器端口。

注意:

- 当“组播 VLAN”功能启用时，本页的配置将失效。

配置步骤：

步骤	操作	说明
1	启用 IGMP 侦听功能	必选操作。在**组播管理>>IGMP 侦听>>基本配置、端口参数**页面，启用交换机的 IGMP 侦听功能和端口的 IGMP 侦听功能。
2	配置 VLAN 的组播参数	可选操作。在**组播管理>>IGMP 侦听>>VLAN 参数**页面，为交换机的各个 VLAN 配置组播参数。 没有配置组播参数的 VLAN，表示没有在该 VLAN 内开启 IGMP 侦听功能，那么该 VLAN 中的组播数据会广播。

8.1.4 组播VLAN

对于传统的组播数据转发方式，当处于不同 VLAN 的用户加入同一个组播组时，组播路由器会为每个包含接收者的 VLAN 复制并转发一份组播数据。这样的组播点播方式，浪费了大量的带宽。

通过配置组播 VLAN，可以有效的解决上述问题。将交换机的端口加入到组播 VLAN 中，使不同 VLAN 内的用户共用一个组播 VLAN 接收组播数据，组播数据只在组播 VLAN 内进行传输，从而节省了带宽。同时由于组播 VLAN 与普通的 VLAN 完全隔离，安全和带宽都得以保证。

配置组播 VLAN 之前，需要在 **802.1Q VLAN** 功能处预先配置一个 VLAN 作为组播 VLAN，并将相应的端口加入此 VLAN 中。组播 VLAN 启用后，在 **VLAN 参数**页面中为其它 VLAN 配置的组播参数将失效，即组播数据不再通过除组播 VLAN 以外的其它 VLAN 转发。

进入页面的方法：组播管理>>IGMP 侦听>>组播 VLAN

组播VLAN

组播VLAN： 启用 禁用

VLAN ID： (2-4094)

路由器端口时间： 秒(60-600，推荐300秒)

成员端口时间： 秒(60-600，推荐260秒)

离开滞后时间： 秒(1-30，推荐1秒)

静态路由端口： 禁用

提交 帮助

注意：

1、创建了组播VLAN 后，所有的IGMP报文都在组播VLAN内处理。

2、必须在VLAN配置页面完成端口的相关VLAN属性配置，组播VLAN才能正常运行。

图 8-7 组播 VLAN

条目介绍：

- **组播 VLAN**

组播 VLAN： 选择是否启用组播 VLAN。

VLAN ID： 填写组播 VLAN 的 VLAN ID。

路由器端口时间： 在所设时间内，如果交换机没有从路由器端口接收到查询报文，就认为该路由器端口失效。推荐 300 秒。

成员端口时间： 在所设时间内，如果交换机没有接收到成员端口发送的报告报文，就认为该成员端口失效。推荐 260 秒。

离开滞后时间： 主机发送离开报文到交换机把该主机端口从组播组中删除的间隔时间。推荐 1 秒。

静态路由端口： 选择静态配置的路由器端口，多用于拓扑稳定的网络中。

注意：

- 路由器端口必须均在组播 VLAN 中，否则成员端口无法收到组播数据。
- 必须在 **802.1Q VLAN** 功能处完成端口的相关 VLAN 属性配置，组播 VLAN 才能正常运行。
- 组播 VLAN 中的成员端口的端口类型只能够为 GENERAL。
- 组播 VLAN 中的路由器端口的端口类型必须配置为 TRUNK 或者是出口规则为“带 tag”的 GENERAL 端口，否则组播 VLAN 内的所有的组播成员端口都无法接收到组播数据。
- 建立了组播 VLAN 后，所有的 IGMP 报文只在组播 VLAN 内处理。

配置步骤：

步骤	操作	说明
1	启用 IGMP 侦听功能	必选操作。在**组播管理>>IGMP 侦听>>基本配置**、**端口参数**页面，启用交换机的 IGMP 侦听功能和端口的 IGMP 侦听功能。
2	创建组播 VLAN	必选操作。在 **VLAN>>802.1Q VLAN** 功能处，创建组播 VLAN，并将所有成员端口和路由器端口加入该 VLAN 中。 ● 配置成员端口的端口类型为 GENERAL。 ● 配置路由端口的端口类型为 TRUNK 或出口规则为“带 tag”的 GENERAL。
3	配置组播 VLAN 的参数	可选操作。进入**组播管理>>IGMP 侦听>>组播 VLAN** 页面，启用组播 VLAN 并配置组播 VLAN 的组播参数。 时间参数建议使用默认值。
4	查看配置情况	若配置成功，则在**组播管理>>IGMP 侦听>>基本配置**页面中的“已启用的 VLAN”条目处，显示组播 VLAN 的 VLAN ID。

8.2 IGMP侦听功能组网应用

➤ 组网需求

组播源通过路由器转发组播数据，组播数据流通过交换机被转发到接收端用户 A 和用户 B。

路由器：WAN 口与组播源相连；LAN 口与交换机相连，且通过 VLAN3 转发数据。

交换机：端口 3 与路由器相连，且通过 VLAN3 转发数据；端口 4 与用户 A 相连，且通过 VLAN4

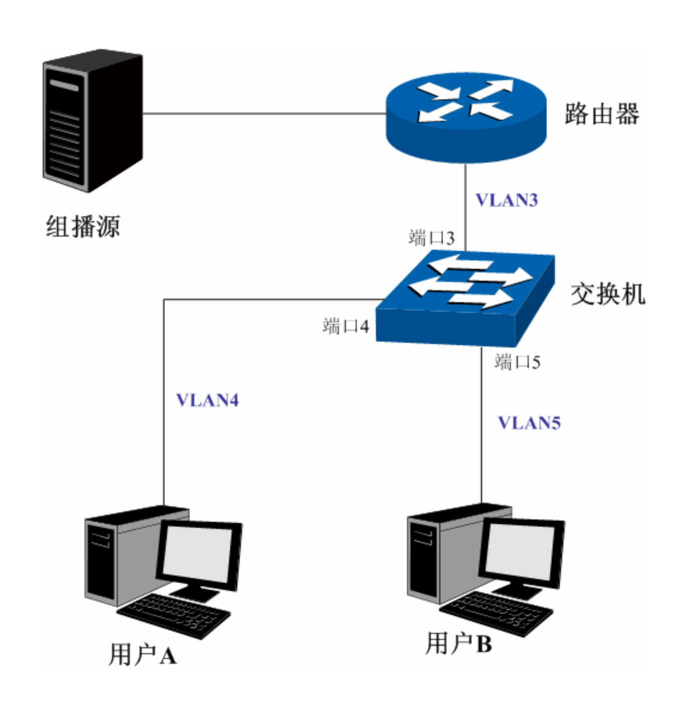
转发数据；端口 5 与用户 B 相连，且通过 VLAN5 转发数据。

用户 A：与交换机的端口 4 相连。

用户 B：与交换机的端口 5 相连。

配置组播 VLAN，使用户 A 和用户 B 通过组播 VLAN 接收组播数据。

➢ 组网图



➢ 配置步骤

配置交换机：

步骤	操作	说明
1	创建 VLAN	在 **VLAN>>802.1Q VLAN** 功能处，创建 VLAN3、4、5，并将 VLAN3 的描述填写为“组播 VLAN”。
2	配置端口属性	在 **VLAN>>802.1Q VLAN** 功能处。 配置端口 3 的端口类型为 GENERAL，出口规则 TAG，并加入 VLAN3、4、5 中。 配置端口 4 的端口类型为 GENERAL，出口规则 UNTAG，并加入 VLAN3、4 中。 配置端口 5 的端口类型为 GENERAL，出口规则 UNTAG，并加入 VLAN3、5 中。
3	启用 IGMG 侦听	在**组播管理>>IGMP 侦听>>基本配置**页面，启用 IGMP 侦听功能。 在**组播管理>>IGMP 侦听>>端口配置**页面，启用端口 3、4、5 的 IGMP 侦听功能。
4	启用组播 VLAN	在**组播管理>>IGMP 侦听>>组播 VLAN** 页面，启用组播 VLAN，并配置组播 VLAN 的 VLAN ID 为 3，其它参数建议使用默认值。

5	检查组播 VLAN	在**组播管理>>IGMP 侦听>>基本配置**页面，“IGMP 侦听信息”处，“已启用的端口”显示为 3、4、5，“已启用的 VLAN”显示为 3。

8.3 组播地址表

在网络中，信息接收者可以加入各自所需的组播组，交换机在转发组播数据时是根据组播地址表来进行的。本功能包括**地址表显示**和**静态地址表**两个配置页面。

8.3.1 地址表显示

在本页可以查看到交换机中已存在的所有组播地址表信息。

进入页面的方法：组播管理>>组播地址表>>地址表显示



图 8-8 地址表显示

条目介绍：

➢ 基本配置

组播 IP： 选择欲查找条目需包含的组播 IP 地址信息。

VLAN ID： 选择欲查找条目需包含的 VLAN ID 信息。

端口： 选择欲查找条目需包含的端口号。

地址类型： 选择欲查找条目需包含的地址类型信息。

- 全部：显示全部组播地址表条目。
- 静态：显示静态组播地址表条目。
- 动态：显示动态组播地址表条目。

➢ 组播 IP 表

组播 IP： 显示组播 IP 地址。

VLAN ID： 显示组播组对应的 VLAN ID。

转发端口： 显示组播组的转发端口。

地址类型： 显示组播 IP 的类型

注意：

- 若改变 **VLAN** 参数或组播 **VLAN** 页面中的参数，交换机都会先清空组播地址表中的动态组播地址，然后再重新学习。

8.3.2 静态地址表

静态组播地址表不是通过 IGMP 侦听学习到的，不受动态组播组及组播过滤的影响，对于某些固定的组播组，可以提高数据传输质量并增加安全性。

进入页面的方法：组播管理>>组播地址表>>静态地址表

新建条目

组播IP：（格式为：225.0.0.1）

VLAN ID：（1-4094）

转发端口：（格式为：1-3,6,8）

添加

查找条目

查找选项：全部 查找

静态组播IP表

选择	组播IP	VLAN ID	转发端口

全选 删除 帮助

当前静态组播IP总数：0

图 8-9 静态地址表

条目介绍：

➢ 新建条目

组播 IP： 填写静态绑定的组播 IP 地址。

VLAN ID： 填写组播 IP 对应的 VLAN ID。

转发端口： 填写组播 IP 的转发端口。

➢ 查找条目

查找选项： 选择静态组播 IP 表的显示规则，可以帮助您快速查找到所需的条目。

- 全部：显示全部静态组播 IP 表条目。
- 组播 IP：设置欲查找条目需包含的组播 IP 地址信息。
- VLAN ID：设置欲查找条目需包含的 VLAN ID 信息。
- 端口 ID：设置欲查找条目需包含的端口。

➢ 静态组播 IP 表

选择： 勾选条目进行删除，可多选。

组播 IP： 显示绑定的组播 IP 地址。

VLAN ID： 显示组播组对应的 VLAN ID。

转发端口： 显示组播组的转发端口。

8.4 组播过滤

在启用了 IGMP 侦听后，可以通过配置组播过滤，来限制端口能加入的组播地址范围，从而限制用户对组播节目的点播。

当用户申请加入某个组播组时，会发送 IGMP 报告报文，该报文到达交换机后，交换机首先检查接收端口上所配置的组播过滤规则，如果此端口可以加入这个组播组，则将这个端口加入到该组播组的地址表中；否则交换机就丢弃该 IGMP 报告报文，这样组播数据就不会转发到该端口，从而控制了用户加入组播组。

8.4.1 过滤地址

本页用来配置需要过滤的组播地址段。

进入页面的方法：组播管理>>组播过滤>>过滤地址

新建条目

过滤地址ID： (1-30)

起始组播IP： （格式为：225.0.0.1）

结束组播IP： （格式为：225.0.0.1）

添加

过滤地址表

过滤地址ID 选择

选择	过滤地址ID	起始组播IP	结束组播IP
☐			

提交 删除 帮助

当前过滤地址总数：0

图 8-10 过滤地址

条目介绍：

➢ 新建条目

过滤地址 ID： 填写过滤地址 ID 号。

起始组播 IP： 填写过滤地址段的起始组播 IP 地址。

结束组播 IP： 填写过滤地址段的结束组播 IP 地址。

➢ 过滤地址表

过滤 ID 选择： 点击<选择>按键，可根据所输过滤地址 ID 号，快速查找条目。

选择： 勾选条目进行删除或修改过滤地址范围，可多选。

过滤地址 ID： 显示过滤地址 ID 号。

起始组播 IP： 显示过滤地址段的起始组播 IP 地址。

结束组播 IP： 显示过滤地址段的结束组播 IP 地址。

8.4.2 端口过滤

本页用来配置端口的组播过滤规则，与“过滤地址”页面想结合，共同实现交换机的组播过滤功能。

进入页面的方法：组播管理>>组播过滤>>端口过滤



图 8-11 端口过滤

条目介绍：

➢ 端口过滤配置

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

选择： 勾选条目配置端口的组播过滤功能，可多选。

端口： 显示交换机的端口号。

过滤： 选择是否启用端口组播过滤功能。

动作模式： 选择当组播地址属于过滤地址范围时，交换机对数据包的处理方式。

- 允许：只有组播地址属于过滤地址范围时，才处理组播报文。
- 拒绝：只处理组播地址不在过滤地址范围内的组播报文。

绑定过滤地址： 配置该端口需要绑定的过滤地址 ID 号。

最多加入组播数： 通过限制端口最多加入组播组数，来避免某些端口占据过多带宽。

LAG： 显示端口当前所属的汇聚组。

注意：

- 组播过滤功能只对启用了 IGMP 侦听的 VLAN 生效。
- 组播过滤功能对静态组播 IP 不生效。
- 一个端口最多只能绑定 5 个过滤地址。

配置步骤：

步骤	操作	说明
1	配置过滤地址段	必选操作。在**组播管理>>组播过滤>>过滤地址**页面，为过滤地址 ID 配置对应的过滤地址段。
2	配置端口的组播过滤规则	必选操作。在**组播管理>>组播过滤>>端口过滤**页面，配置端口的组播过滤规则。

8.5 报文统计

在本页可以查看交换机各端口的组播报文流量信息，便于监控网络中 IGMP 报文。

进入页面的方法：**组播管理>>报文统计**



端口	查询报文	报告报文(V1)	报告报文(V2)	报告报文(V3)	离开报文	错误报文
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0

图 8-12 报文统计

条目介绍：

➢ 自动刷新

自动刷新： 选择是否启用自动刷新功能。

刷新周期： 填写自动刷新的时间周期。默认为 5 秒。

➢ **IGMP** 报文统计

端口选择： 点击<选择>按键，可根据所输端口号，快速选择相应端口。

端口： 显示交换机的端口号。

查询报文数： 显示端口接收到的查询报文的数目。

报告报文(V1)： 显示端口接收到的 IGMPv1 报告报文的数目。

报告报文(V2)： 显示端口接收到的 IGMPv2 报告报文的数目。

报告报文(V3)： 显示端口接收到的 IGMPv3 报告报文的数目。

离开报文： 显示端口接收到的离开报文的数目。

错误报文： 显示端口接收到的错误报文的数目。

回目录

第9章 服务质量

服务质量模块主要用于流量控制管理和优先级配置，针对各种网络应用的不同需求，为其提供不同的服务质量，对带宽资源进行最优配置，从而提供更高质量的网络服务体验，包括 **QoS 配置**、**流量管理**以及**语音 VLAN** 三个部分。

9.1 QoS配置

QoS(Quality of Service 即服务质量)功能用以提高网络传输的可靠性，并为您提供更高质量的网络服务体验。在传统的 IP 网络中，所有的报文都被无区别的等同对待，网络尽最大的努力（Best-Effort）发送报文，但对时延、可靠性等性能不能提供任何保证。伴随着网络技术、多媒体技术的飞速发展，IP 网在现有的 www, FTP, E-mail 等服务的基础上，越来越多承载交互式多媒体通信业务如电视会议、远程教学、视频点播、可视电话等，而每种业务要求的传输时延、可变迟延、吞吐量和丢包率都不同。因此，为用户各种业务提供不同的服务质量（QoS)成为 Internet 发展的重要挑战。

通常所说的 QoS，是针对各种网络应用的不同需求，为其提供不同的服务质量，如提供专用带宽，减少报文丢失率，降低报文传送时延及时延抖动等。即在带宽不充裕的情况下，对各种服务流量占用带宽的矛盾做一个平衡。

➢ **QoS 工作原理**

本交换机通过在入口阶段对数据流进行分类，然后在出口阶段将不同类型的数据流映射到不同优先级的队列，最后依据调度模式来决定不同优先级队列的数据包被转发的方式，从而实现了 QoS 功能。

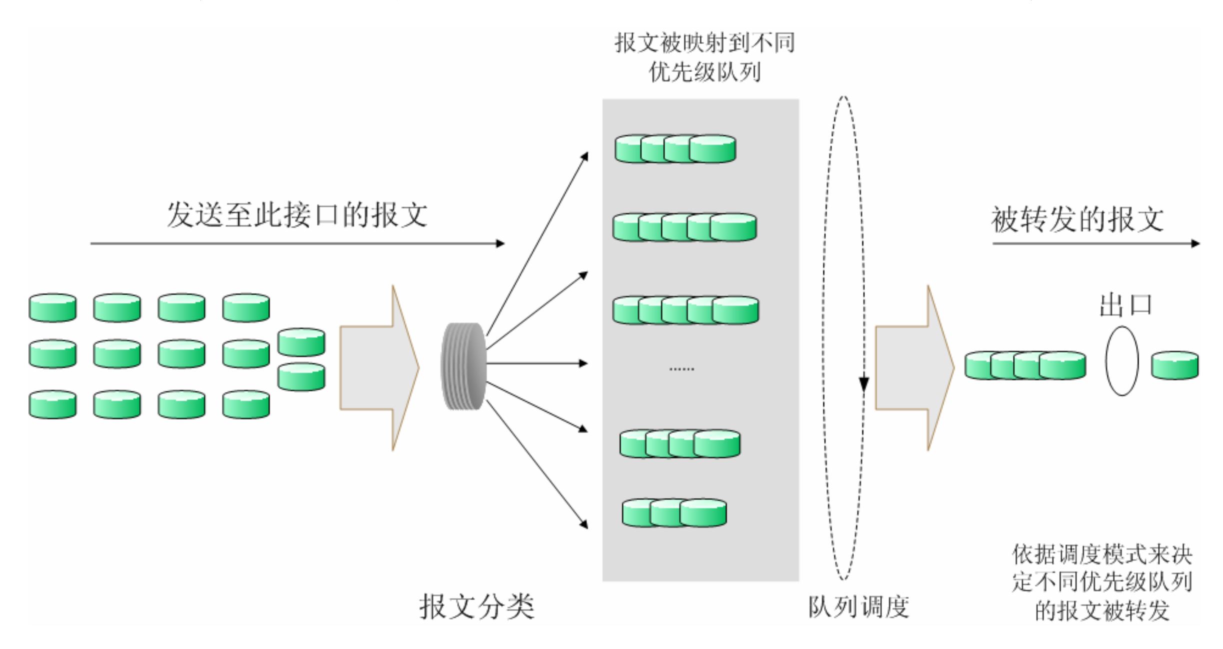


图 9-1 QoS 工作原理

- 报文分类：依据一定的匹配规则识别出对象。
- 映射：用户可以根据优先级模式，将进入交换机的报文映射到不同的优先级队列中。本交换机提供三种优先级模式：基于端口的优先级、802.1P 优先级和 DSCP 优先级。

- 队列调度：当网络拥塞时，必须解决多种数据流同时竞争使用资源的问题，通常采用队列调度加以解决。本交换机共提供了四种调度模式，分别是严格优先级模式（SP）、加权轮询优先级模式（WRR）、SP+WRR 模式和无优先级模式（Equ）。

➢ 优先级模式

本交换机共有基于端口的优先级、IEEE 802.1P 优先级和 DSCP 优先级三种模式。其中基于端口的优先级是默认被启用的，其它两种优先级模式可供选择。

1. 基于端口的优先级

端口优先级只是端口的一个属性值，在设置了端口优先级后，数据流会根据入端口的 CoS 值以及 802.1P 中 CoS 到队列之间的映射关系来确定数据流的出口队列。

2. 802.1P 优先级

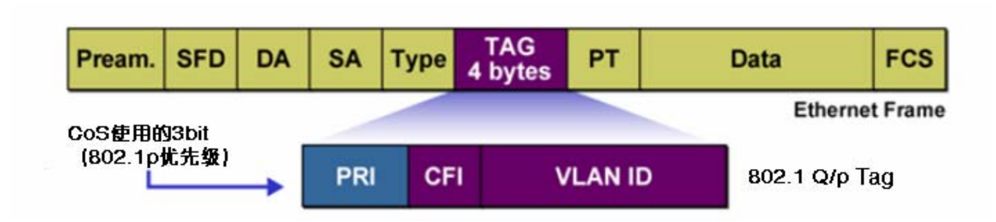


图 9-2 802.1Q 的帧格式

如图所示，每一个 802.1Q Tag 中都有一个 Pri 域，该域由三个 bit 为组成，取值范围是 0~7。802.1P 优先级就是根据 Pri 的域值来决定数据帧的优先级。通过交换机的配置页面可配置不同的 Pri 域对应不同的优先级，交换机发送数据帧时，会根据数据帧的 Tag 决定发送的优先级。对于 Untagged 帧，交换机则按照该入口端口的默认优先级对数据帧进行 QoS 处理。

3. DSCP 优先级

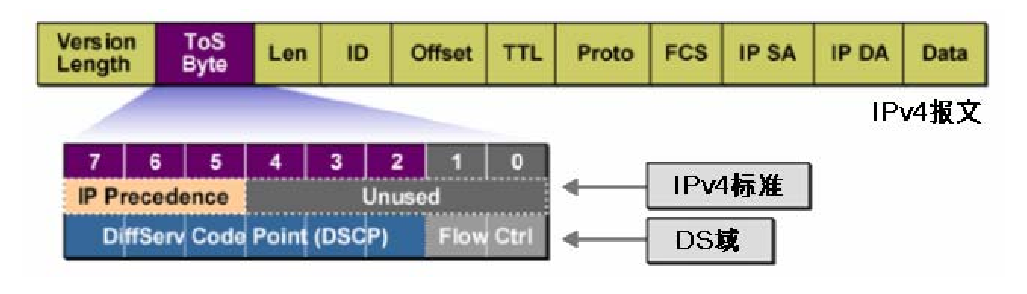


图 9-3 IP 报文

如图所示，IP 报文头部的 ToS（Type of Service，服务类型）字段共有 8bit，可以表征不同优先级特征的报文，前 3 个 bit 表示的是 IP 的优先级，取值范围是 0~7。RFC2474 重新定义了 IP 报文头部的 ToS 域，称之为 DS 域。其中 DSCP（Differentiated Services Codepoint，差分服务编码点）优先级用该域的前 6 个 bit（0～5bit）表示，取值范围为 0～63，后 2 个 bit（6、7bit）是保留位。通过交换机的配置页面，可以配置不同的 DS 字段对应不同的优先级，交换机发送 IP 包时，会根据 IP 包的 DS 域决定发送的优先级。对于非 IP 包，交换机则根据是否启用 802.1P 优先级以及数据帧是否带有 Tag 来决定采用哪种优先级模式。

注意：

- 当启用 802.1P 优先级时，根据数据包是否带有 802.1Q Tag 确定使用哪种优先级模式。对于带

有 Tag 的数据包，应用 802.1P 优先级；否则应用端口优先级。当启用 DSCP 优先级的时候，如果数据包是 IP 包，则应用 DSCP 优先级；对于非 IP 包，交换机则根据是否启用 802.1P 优先级以及数据帧是否带有 Tag 来决定采用哪种优先级模式。

➢ **调度模式**

在网络拥塞时，通常采用队列调度来解决多个数据流同时竞争使用资源的问题。本交换机共实现了 4 个调度队列—TC0 到 TC3，其中 TC0 对应最低优先级的队列，TC3 对应到最高优先级的队列。同时，本交换机共提供了四种调度模式，分别是严格优先级模式（SP）、加权轮询优先级模式（WRR）、SP+WRR 模式和无优先级模式（Equ）。

1. SP-Mode：严格优先级模式。SP 模式的调度算法是交换机优先转发当前优先级最高的数据帧，等最高优先级数据帧全部转发完后，再转发次高级优先级的数据帧。本交换机有 4 个出口队列，依次为 TC0-TC3，在 SP 队列模式下他们的优先级依次升高，TC3 有最高优先级。SP 队列的缺点是，在拥塞发生时，如果较高优先级队列中长时间有报文存在，那么低优先级队列中的报文就会由于得不到服务而“饿死”。

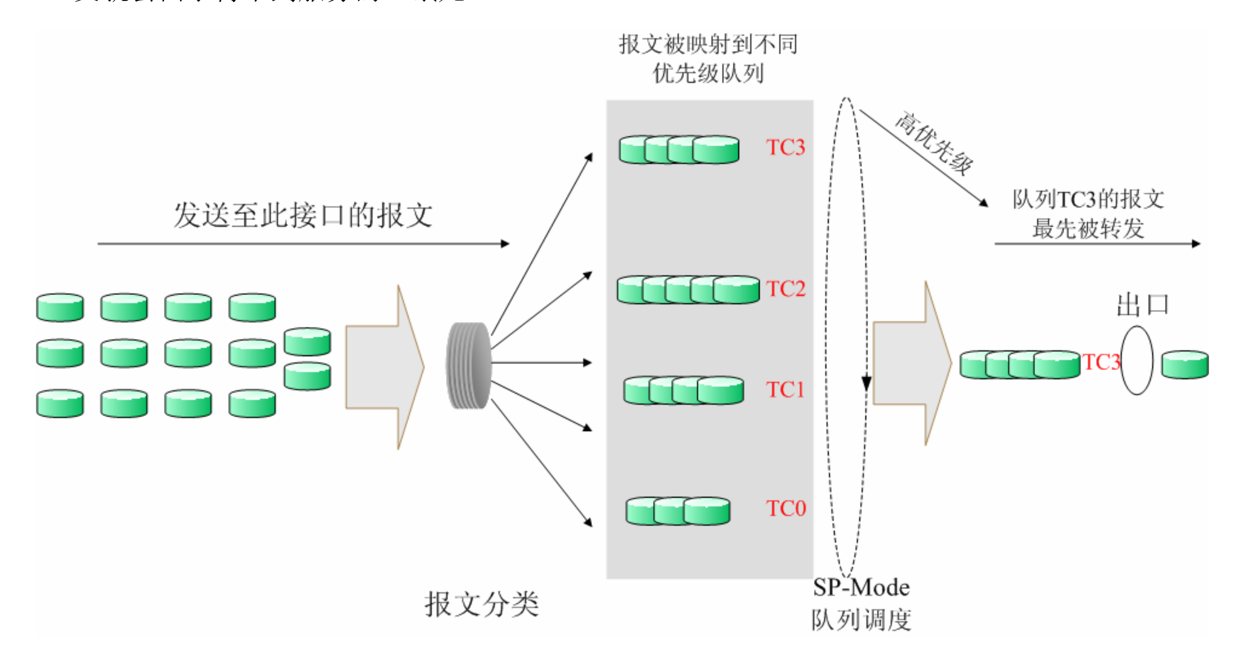


图 9-4 严格优先级模式

2. WRR-Mode：WRR 优先级模式。WRR 模式的调度算法是在队列之间按权重比值进行轮流调度，以保证每个队列都得到一定的服务时间，加权值表示获取资源的比重。WRR 队列避免了采用 SP 调度时低优先级中的报文可能长时间得不到服务的缺点，并且虽然多个队列调度是轮询进行的，但是对每个队列不是固定的分配服务时间，如果队列为空则马上更换下一个队列调度，这样可以充分利用带宽资源。TC0-TC3 的默认权重比是 1:2:4:8。

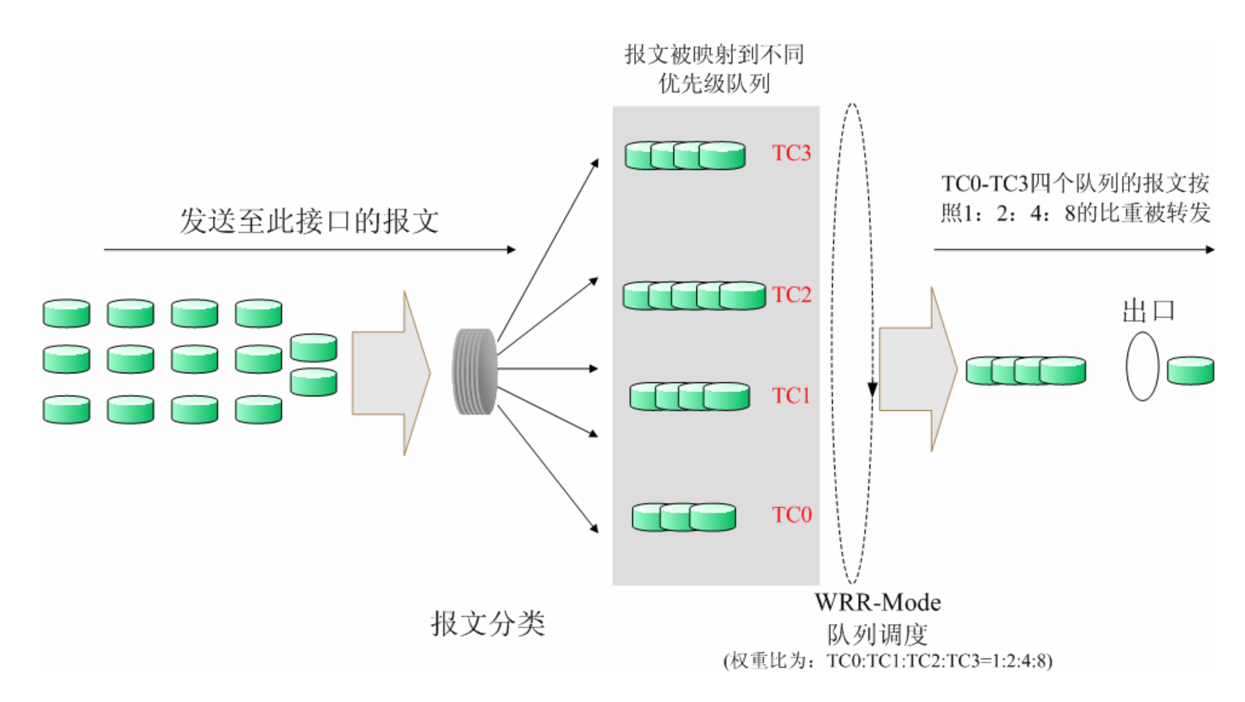


图 9-5 WRR 优先级模式

3. SP+WRR-Mode：SP+WRR 优先级模式，这种模式是前两种模式的混合。在这种模式下，交换机提供了两个调度组，分别是 SP 组和 WRR 组。其中 SP 组和 WRR 组之间遵循的是严格优先级调度规则，而 WRR 组内部队列遵循的是 WRR 调度模式。在该调度模式下 TC3 属于 SP 组；TC0、TC1、TC2 属于 WRR 组，权重比是 1：2：4。这样在调度的时候首先是 TC3 按照 SP 的调度模式独自占用带宽，然后是 WRR 组的成员 TC0、TC1、TC2 按照权重比 1：2：4 的比例占用带宽。

4. Equ-Mode：无优先级模式。这种模式下所有队列公平的占用带宽，实际上这是 WRR 模式的一种特殊情况，所有的队列权重比是 1:1:1:1。

本交换机实现了基于端口、基于 802.1P 和基于 DSCP 的三种优先级模式以及四个队列调度模式。端口优先级以 CoS 0,CoS1…CoS 7 表示。QoS 配置功能包括**基本配置**、**调度模式**、**802.1P**、**DSCP** 四个配置页面。

9.1.1 基本配置

在基本配置页面中，您可以进行基于端口优先级的配置。

进入页面的方法：服务质量>>QoS 配置>>基本配置

端口优先级配置

选择	端口	优先级	LAG
☐		CoS 0	
☐	1	CoS 0	---
☐	2	CoS 0	---
☐	3	CoS 0	---
☐	4	CoS 0	---
☐	5	CoS 0	---
☐	6	CoS 0	---
☐	7	CoS 0	---
☐	8	CoS 0	---
☐	9	CoS 0	---
☐	10	CoS 0	---

提交 帮助

注意：
端口优先级只是端口的一个属性值，在设置了端口优先级后，数据流会根据入端口的CoS值以及802.1P中CoS到TC之间的映射关系来确定数据流的出口队列。

图 9-6 基本配置

条目介绍：

➢ 端口优先级配置

选择：	勾选端口配置端口优先级，可多选。
端口：	显示交换机的物理端口。
优先级：	配置端口的所属优先级等级。
LAG：	显示当前端口所属的 LAG 组。

注意：

- 在此页面完成配置之后，需进入**调度模式**页面选择调度模式才能完成 QoS 功能的配置。

配置步骤：

步骤	操作	说明
1	进入页面	
2	选择端口进行配置	勾选所需端口，可多选。
3	选择端口的优先级	可选操作，可选择 CoS 0-CoS 7。
4	选择调度模式	必选操作。进入调度模式页面选择调度模式。

9.1.2 调度模式

在本页面可以进行交换机调度模式的选择。在网络拥塞时，通常采用队列调度来解决多个数据流同时竞争使用资源的问题。交换机将根据设置的优先级队列和队列调度算法来控制报文的转发次序。本交换机以 TC0,TC1…TC3 表示不同的优先级队列。

进入页面的方法：服务质量>>QoS 配置>>调度模式

调度模式配置

调度模式： Equ-Mode

提交

帮助

图 9-7 调度模式

条目介绍：

➢ 调度模式配置

SP-Mode： 严格优先级模式。在此模式下，高优先级队列会占用全部带宽，只有在高优先级队列为空后，低优先级队列才进行数据转发。

WRR-Mode： 加权轮询优先级模式。在此模式下，所有优先级队列按照预先分配的权重比同时发送数据包。TC0 到 TC3 的权重比值是 1：2：4：8。

SP+WRR-Mode： SP+WRR 模式，这种队列调度模式是前两种模式的混合。在此模式下，交换机提供了两个调度组，分别是 SP 组和 WRR 组。其中 SP 组和 WRR 组之间遵循的是严格优先级调度规则，而 WRR 组内部队列遵循的是 WRR 调度模式。
在该调度模式下 TC3 属于 SP 组；TC0、TC1、TC2 属于 WRR 组，权重比是 1：2：4。这样在调度的时候首先是 TC3 按照 SP 的调度模式独自占用带宽，然后是 WRR 组的成员 TC0、TC1、TC2 按照权重比 1：2：4 的比例占用带宽。

Equ-Mode： 无优先级模式。在此模式下所有队列公平的占用带宽，所有的队列权重比是 1：1：1：1。

9.1.3 802.1P

在802.1P配置页面中，您可以进行802.1P优先级的配置。802.1P对802.1Q tag中的Pri字段进行了的定义，利用该字段可以将数据包划分为8个优先级。开启802.1P 优先级后，交换机根据数据包是否带有802.1Q tag来确定所使用的优先级模式。对于带有tag 的数据包，应用802.1P优先级；否则应用基于端口的优先级。

进入页面的方法：服务质量>>QoS 配置>>802.1P



图 9-8 802.1P 优先级

条目介绍：

- **优先级配置**

802.1P 优先级： 选择是否启用 802.1P 优先级。

- **优先级等级**

优先级 Tag： IEEE802.1P 协议里规定的 8 个优先级等级。

优先级等级： 对应不同等级的优先级队列。以 TC0,TC1…TC3 表示。

注意：

- 在此页面完成配置之后，需进入**调度模式**页面选择调度模式才能完成 QoS 功能的配置。

配置步骤：

步骤	操作	说明
1	进入页面	
2	启用 802.1P 优先级模式	必选操作。缺省状态下，802.1P 功能为禁用。
3	将 802.1P 优先级对应至优先级等级队列	必选操作。选择 802.1P 优先级的同时选择相应的优先级等级队列。
4	选择调度模式	必选操作。进入调度模式页面选择调度模式。

9.1.4 DSCP

在 DSCP 配置页面中，您可以进行 DSCP 优先级的配置。DSCP(DiffServ Code Point，区分服务编码点)是 IEEE 对 IP ToS 字段的重定义，利用该字段可以将 IP 报文划分为 64 个优先级。开启 DSCP 优先级后，如果转发的数据包是 IP 报文，则交换机应用 DSCP 优先级；对于非 IP 报文，交换机则根据是否启用 802.1P 优先级以及数据帧是否带有 tag 来决定采用哪种优先级模式。



图 9-9 DSCP 优先级

条目介绍：

➢ 优先级配置

DSCP 优先级： 选择是否启用 DSCP 优先级。

➢ 优先级等级

DSCP： 根据 IP 包的 DS 域决定的优先级。优先级级别从 0 到 63。

优先级等级： 对应不同等级的优先级队列。以 TC0,TC1…TC3 表示。

注意：

● 在此页面完成配置之后，需进入**调度模式**页面选择调度模式才能完成 QoS 功能的配置。

配置步骤：

步骤	操作	说明
1	进入页面	
2	启用 DSCP 优先级模式	必选操作。缺省状态下，DSCP 功能为禁用。
3	将 DSCP 优先级对应至优先级等级队列	必选操作。选择 DSCP 优先级的同时选择相应的优先级等级队列。
4	选择调度模式	必选操作。进入调度模式页面选择调度模式。

9.2 流量管理

流量管理用于限制交换机端口的带宽和广播流量，保证网络正常有效的运行，包括**带宽控制**和**风暴抑制**两个配置页面。

9.2.1 带宽控制

带宽控制是通过设定端口可用带宽，来控制端口的输入/输出数据传输速率，从而合理地分配和利用网络带宽。

进入页面的方法：服务质量>>流量管理>>带宽控制



图 9-10 带宽控制

条目介绍：

➢ 带宽控制

端口选择：	点击<选择>按键，可根据所输端口号，快速选中相应端口。
选择：	勾选端口以配置端口带宽，可多选也可不选。
入口带宽(bps)：	配置端口接收数据时的带宽，可选择下拉列表中提供的带宽，也可选择“手动输入”或“禁用”选项。若选择“手动输入”选项，则系统将会自动选择与填写的数值最相近的 64Kbps 的整数倍值作为入口带宽的输入值；若选择“禁用”选项，则该端口的入口带宽控制会被取消，该端口的入口带宽将恢复为最大带宽。

出口带宽(bps)： 配置端口转发数据时的带宽，可选择下拉列表中提供的带宽，也可选择“手动输入”或“禁用”选项。若选择“手动输入”选项，则系统将会自动选择与所填写的数值最相近的 64Kbps 整数倍值作为出口带宽的输入值；若选择“禁用”选项，则该端口的出口带宽控制会被取消，该端口的出口带宽将恢复为最大带宽。

LAG： 显示端口当前所属的汇聚组。勾选某个汇聚组的成员端口时，会自动选择所有该汇聚组成员，以保证同一汇聚组中所有成员的端口风暴抑制参数一致。

注意：

- 若端口已启用广播风暴抑制，再启用入口带宽限制将使其失效。
- 在一个或多个端口上启用出口带宽限制时，建议将各端口的流量控制禁用，以保证交换机的正常工作。

9.2.2 风暴抑制

广播风暴是指网络上的广播帧由于不断被转发导致数量急剧增加而影响正常的网络通讯，严重降低网络性能。广播风暴的判断标准为一个端口是否在短时间内连续收到许多个广播帧。风暴抑制是指用户可以限制端口上允许接收的广播流量大小，当该类流量超过用户设置的阈值后，系统将丢弃超出流量限制的广播帧，防止广播风暴的发生，从而保证网络的正常运行。

本交换机可以对三种常见的广播帧（广播包、组播包、UL 包）进行限制。

进入页面的方法：服务质量>>流量管理>>风暴抑制



选择	端口	广播包抑制(bps)	组播包抑制(bps)	UL包抑制(bps)	LAG
☐		100K	100K	100K	
☐	1	---	---	---	---
☐	2	---	---	---	---
☐	3	---	---	---	---
☐	4	---	---	---	---
☐	5	---	---	---	---
☐	6	---	---	---	---
☐	7	---	---	---	---
☐	8	---	---	---	---
☐	9	---	---	---	---
☐	10	---	---	---	---
☐	11	---	---	---	---
☐	12	---	---	---	---

图 9-11 风暴抑制

条目介绍：

➢ 风暴抑制

端口选择：	点击<选择>按键，可根据所输端口号，快速选中相应端口。
选择：	勾选端口以配置风暴抑制参数，可多选也可不选。
广播包抑制(bps)：	对由普通广播引起的风暴进行抑制。配置广播包的最大接收速度，可选择 100K、200K、500K，1M、2M、4M、5M，10M、20M、40M、50M，超出流量部分的数据包将被丢弃。选择“禁用”选项时将关闭相应端口的广播包抑制。
组播包抑制(bps)：	对由组播引起的风暴进行抑制。配置组播包的最大接收速度，可选择 100K、200K、500K，1M、2M、4M、5M，10M、20M、40M、50M，超出流量部分的数据包将被丢弃。选择“禁用”选项时将关闭相应端口的组播包抑制。
UL 包抑制(bps)：	交换机对未学习到地址的单播包（UL 包）进行广播，对由此引起的风暴进行控制。配置 UL 包的最大接收速度，可选择 100K、200K、500K，1M、2M、4M、5M，10M、20M、40M、50M，超出流量部分的数据包将被丢弃。选择“禁用”选项时将关闭相应端口的 UL 包抑制。
LAG：	显示端口当前所属的汇聚组。勾选某个汇聚组的成员端口时，会自动选择所有该汇聚组成员，以保证同一汇聚组中所有成员的端口风暴抑制参数一致。

注意：

- 若端口已启用入口带宽限制，再启用广播风暴抑制将使其失效。

9.3 语音VLAN

语音VLAN是为语音数据流而专门划分的VLAN。通过划分语音VLAN可以使语音数据自动被划分到语音VLAN中进行传输，便于对语音流进行有针对性的QoS（Quality of Service，服务质量）配置，提高语音流量的传输优先级，保证通话质量。

➢ 语音数据流识别方法

本交换机可以根据数据包中的源MAC地址字段来判断该数据流是否为语音数据流。源MAC地址符合系统设置的语音设备OUI（Organizationally Unique Identifier，全球统一标识符）地址的报文被认为是语音数据流，被划分到语音VLAN中传输。

OUI（Organizationally Unique Identifier）是MAC地址的前24位（二进制），是IEEE（Institute of Electrical and Electronics Engineers，电气和电子工程师学会）为不同设备供应商分配的一个全球唯一的标识符，从OUI地址可以判断出该设备是哪一个厂商的产品。下表是常见语音设备商家产品的OUI地址，已在本交换机中设置为缺省OUI地址，设定不同的掩码可以调节交换机对MAC地址匹配的深度。

序号	OUI 地址	设备商家
1	00-01-E3-00-00-00	Siemens phone
2	00-03-6B-00-00-00	Cisco phone

3	00-04-0D-00-00-00	Avaya phone
4	00-60-B9-00-00-00	Philips/NEC phone
5	00-D0-1E-00-00-00	Pingtel phone
6	00-E0-75-00-00-00	Polycom phone
7	00-E0-BB-00-00-00	3com phone

表9-1 本交换机中缺省 OUI 地址

➢ **端口的语音 VLAN 模式**

端口的语音VLAN模式包括自动模式和手动模式，是指端口加入语音VLAN的方式。

自动模式：系统利用IP电话上电时发出的协议报文（UNTAG报文），通过识别报文的源MAC，匹配OUI地址，匹配成功后，系统将自动把语音报文的输入端口加入语音VLAN，配置报文的优先级。在设备上可以设置语音VLAN的老化时间。如果在老化时间内，系统没有从输入端口收到任何语音报文，系统将把该端口从语音VLAN中删除。端口的添加/删除过程由系统自动实现。

手动模式：需要手动把IP电话接入端口加入语音VLAN中，再通过识别报文的源MAC，匹配OUI地址，匹配成功后，系统将下发ACL规则、配置报文的优先级。

在实际应用中，端口模式的设置需要结合语音设备发出的报文形式和端口的链路类型来进行设置，具体请参考下表。

端口语音VLAN 模式	语音流类型	端口链路类型及处理方式
自动模式	TAG 语音流	ACCESS：不支持。
		TRUNK：支持，但接入端口的缺省 VLAN 不能是语音 VLAN。
		GENERAL：支持，但接入端口的缺省 VLAN 不能是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 TAG。
	UNTAG 语音流	ACCESS：支持。
		TRUNK：不支持。
		GENERAL：支持，但接入端口的缺省 VLAN 不能是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 UNTAG。
手动模式	TAG 语音流	ACCESS：不支持。
		TRUNK：支持，但接入端口的缺省 VLAN 不能是语音 VLAN。
		GENERAL：支持，但接入端口的缺省 VLAN 不能是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 TAG。
	UNTAG 语音流	ACCESS：支持。
		TRUNK：不支持。
		GENERAL：支持，但接入端口的缺省 VLAN 必须是语音 VLAN，同时接入端口在语音 VLAN 中的出口规则必须为 UNTAG。

表9-2 端口模式与语音数据流的处理关系

➢ 语音 **VLAN** 安全模式

当端口使能了语音VLAN功能后，通过配置端口的安全模式还可以过滤数据流。若启用安全模式，则端口只转发语音数据包，对于其它源MAC地址不匹配OUI地址的数据包，端口将直接丢弃。若禁用安全模式，则端口转发所有数据包。

安全模式	报文类型	处理方式
启用	UNTAG 报文	当该报文源 MAC 地址是可识别的 OUI 地址时，允许该报文在语音 VLAN 内传输，否则将该报文丢弃。
	带有语音 VLAN TAG 的报文	
	带有其它 VLAN TAG 的报文	根据指定端口是否允许该 VLAN 通过来对报文进行转发和丢弃的处理，不受语音 VLAN 安全模式的影响。
禁用	UNTAG 报文	不对报文的源 MAC 地址进行检查，所有报文均可在语音 VLAN 内传输。
	带有语音 VLAN TAG 的报文	
	带有其它 VLAN TAG 的报文	根据指定端口是否允许该 VLAN 通过来对报文进行转发和丢弃的处理，不受语音 VLAN 安全模式的影响。

表9-3 安全模式与各种数据的处理关系

注 意：

- 除非有特殊需求，请不要在语音 VLAN 中同时传输语音和其它业务数据。

9.3.1 全局配置

在全局配置页面中，可以设置语音VLAN的全局参数，包括VLAN ID、老化时间、以及语音数据包的传输优先级等等。

进入页面的方法：服务质量>>语音 VLAN>>全局配置

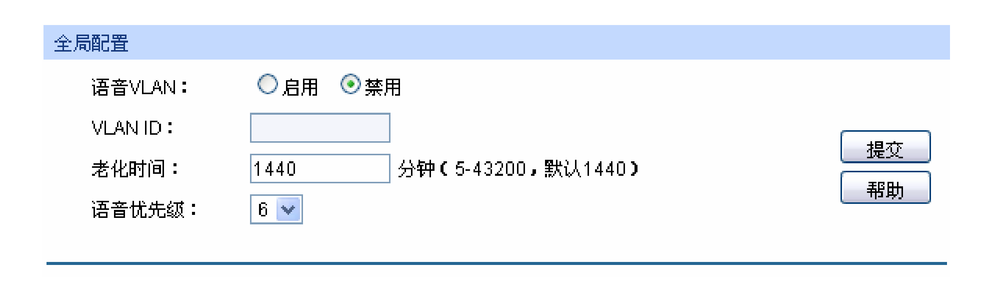


图9-12 语音 VLAN 全局配置

条目介绍：

➢ 全局配置

语音 VLAN： 选择是否启用语音 VLAN 功能。

VLAN ID： 输入该语音 VLAN 的 VLAN ID。

老化时间： 设置自动模式下的端口成员在 OUI 地址老化后的存活时间。

语音优先级： 选择端口发送语音数据包时的数据传输优先级。

9.3.2 端口配置

在启用语音 VLAN 功能之前，需要在端口配置页面中配置各端口的功能参数。

进入页面的方法：服务质量>>语音 VLAN>>端口配置



端口配置

端口 [ ] 选择

选择	端口	成员模式	安全模式	成员状态	LAG
☐					
☐	1	自动	禁用	退出	---
☐	2	自动	禁用	退出	---
☐	3	自动	禁用	加入	---
☐	4	自动	启用	加入	---
☐	5	手动	启用	退出	LAG1
☐	6	手动	启用	退出	LAG1
☐	7	手动	禁用	退出	LAG1
☐	8	手动	禁用	退出	---
☐	9	手动	禁用	退出	---
☐	10	手动	禁用	退出	LAG2
☐	11	手动	禁用	退出	LAG2
☐	12	手动	禁用	退出	---
☐	13	手动	禁用	退出	---
☐	14	手动	禁用	退出	---

提交 帮助

图9-13 语音 VLAN 端口配置

注意：

- 若 LAG 组成员端口要启用语音 VLAN 功能，请保持端口的成员模式和端口模式一致。
- 当端口为语音 VLAN 的成员端口时，修改该端口的成员模式为“自动”，此端口首先会退出语音 VLAN，直到收到语音数据时再自动加入语音 VLAN。

条目介绍：

➢ 端口配置

端口选择： 点击<选择>按键，可根据所输端口号快速选择相应条目。

选择： 勾选端口配置端口的语音 VLAN 参数，可多选。

端口： 显示交换机的端口号。

成员模式： 设置端口加入语音 VLAN 的方式，有手动和自动两种方式。

- 自动：交换机根据端口是否收到语音数据自动维护端口加入或退出语音 VLAN。
- 手动：请根据需要手动设置端口加入或退出语音 VLAN。

安全模式： 设置端口转发数据包的模式。

- 禁用：端口转发所有数据。
- 启用：端口只转发语音数据。

成员状态： 显示端口当前在语音 VLAN 中的状态。

LAG： 显示端口当前所属的汇聚组。

9.3.3 OUI配置

本交换机支持新建 OUI 条目，将特殊语音设备的 MAC 地址添加到交换机支持的 OUI 信息中，并以此 OUI 地址判断数据是否是语音数据。当交换机接收到数据包时，将分析数据包并判断是否是语音数据，如果是语音数据则将该端口自动添加到语音 VLAN 中。

进入页面的方法：服务质量>>语音 VLAN>>OUI 配置

新建条目

OUI地址：		（格式为：00-00-00-00-00-01）	
OUI掩码：	FF-FF-FF-00-00-00	（默认为：FF-FF-FF-00-00-00）	添加
OUI描述：		（1-16个字符）	

OUI列表

选择	OUI地址	OUI掩码	OUI描述
当前OUI列表为空			

全选 删除 帮助

图9-14 语音 VLAN OUI 配置

条目介绍：

➢ 新建条目

OUI 地址： 输入语音设备的 OUI 地址。

OUI 掩码： 输入 OUI 地址掩码，常见为 FF-FF-FF-00-00-00。

OUI 描述： 对此 OUI 进行描述，以便区分不同 VoIP 设备。

➢ OUI 列表

OUI 地址： 显示语音设备的 OUI 地址。

OUI 掩码： 显示语音设备的 OUI 地址掩码。

OUI 描述： 显示此 OUI 的描述信息。

语音 VLAN 配置步骤：

步骤	操作	说明
1	设置端口类型	必选操作。在**VLAN>>802.1Q VLAN>>端口配置**页面根据端口连接的设备设置端口类型，并根据表9-2设置语音设备连接端口的端口类型。

2	创建 VLAN	必选操作。在 **VLAN>>802.1Q VLAN>>VLAN 配置**页面中点击<新建>按键创建 VLAN，请输入 VLAN ID 并对其进行描述，在此页面中请同时勾选 VLAN 包含的端口。
3	添加 OUI 地址	可选操作。在**服务质量>>语音 VLAN>>OUI 配置**页面中的查看交换机是否支持相应的 OUI 模板，若不支持请在此页面中添加。
4	使能端口语音 VLAN 特性	必选操作。在**服务质量>>语音 VLAN>>端口配置**页面设置语音 VLAN 中各端口的功能参数。
5	使能语音 VLAN	必选操作。在**服务质量>>语音 VLAN>>全局配置**页面中使能语音 VLAN 功能，并设置全局参数。

回目录

第10章 访问控制

随着网络规模的扩大以及流量的增加，如何有效地控制网络安全和分配带宽已成为网络管理的重要内容。ACL（Access Control List，访问控制列表）功能，通过配置报文的匹配规则和处理方式来实现对数据包的过滤功能，从而有效防止非法用户对网络的访问。另外 ACL 功能也可以控制流量，节约网络资源。ACL 功能对网络安全的控制提供了很大的方便。

在本交换机中，ACL 功能可以对数据包的 L2-L4 层的协议字段进行匹配。通过定义时间段可以设置 ACL 规则的生效时间，配置 policy 可以对匹配了 ACL 规则的数据包进行处理。

10.1 时间段配置

当用户配置的 ACL 规则需要在特定时间段生效时，可以先配置时间段，然后设置 ACL 规则直接引用该时间段即可。ACL 规则只在指定的时间段内生效，从而实现基于时间段的 ACL 过滤。

本交换机可设置的时间段包括绝对时间、周期时间和节假日。绝对时间可以设置在自然日内的生效日期，周期时间则可以设置在每周的固定工作日生效，同时可以根据需要设置节假日来应对某些特殊意义的日期。在每个时间段内，还可以设置四个小的时间片段使生效时间更灵活。

本功能包括**时间段列表**、**新建时间段**和**节假日定义**三个配置页面。

10.1.1 时间段列表

在时间段列表页面，可以查看和编辑当前已添加的时间段信息。

进入页面的方法：访问控制>>时间段配置>>时间段列表



时间段列表

选择	序号	时间段名称	时间片段1	时间片段2	时间片段3	时间片段4	应用模式	操作
☐	1	HN	18:00-24:00	---	---	---	周期&绝对	编辑 | 查看
☐	2	CC	20:00-24:00	---	---	---	周期	编辑 | 查看

全选 删除 帮助

图 10-1 查看时间段列表

条目介绍：

➢ 时间段列表

选择：	选择时间段条目进行删除。
序号：	显示时间段条目的序号。
时间段名称：	显示时间段的名称。
时间片段：	显示时间段中的时间片段。
应用模式：	显示时间段的应用模式。
操作：	点击相应按键可以查看或编辑相应时间段的详细配置信息。

10.1.2 新建时间段

在新建时间段页面，可以添加时间段信息。

进入页面的方法：访问控制>>时间段配置>>新建时间段

时间段定义
时间段名称：
假日
绝对时间 起始日期：2000 / 01 / 01 结束日期：2000 / 01 / 01
周期 星期一 星期二 星期三 星期四 星期五 星期六 星期日

时间片段
起始时间：00 : 00
结束时间：24 : 00
添加

时间片段列表

序号	起始时间	结束时间	操作

提交 帮助

图 10-2 创建时间段

注意：

- 在此页面中，请先配置时间片段，再定义时间段，否则无法配置成功。

条目介绍：

➢ 时间段定义

时间段名称： 填写时间段的名称，便于区分各个时间段的信息。

节假日： 配置时间段的节假日模式。只有当系统日期在节假日内时，基于该时间段的 ACL 规则才能生效。

绝对时间： 配置时间段的绝对时间模式。只有当系统日期在绝对时间内，基于该时间段的 ACL 规则才能生效。

周期： 配置时间段的周期模式。只有当系统日期在周期时间内，基于该时间段的 ACL 规则才能生效。

➢ 时间片段

起始时间： 配置时间段中时间片段的起始时间。

结束时间： 配置时间段中时间片段的结束时间。

➢ 时间片段列表

序号： 显示时间片段的序号。

起始时间： 显示时间段中时间片段的起始时间。

结束时间： 显示时间段中时间片段的结束时间。

操作： 点击删除即可删除相应的时间片段。

10.1.3 节假日定义

节假日定义可以提供与工作日不同的安全访问控制策略。在本页面，可以根据工作安排自行定义节假日。

进入页面的方法：访问控制>>时间段配置>>节假日定义

节假日定义

起始日期： 01 / 01

结束日期： 01 / 01 添加

假日名称：

节假日列表

选择	序号	假日名称	起始日期	结束日期

全选 删除 帮助

图 10-3 节假日定义

条目介绍：

- 节假日定义

起始日期：	配置节假日起始日期。
终止日期：	配置节假日终止日期。
假日名称：	填写假日名称，请输入英文字符。

- 节假日列表

选择：	选择节假日条目进行删除。
序号：	显示节假日条目的序号。
假日名称：	显示假日名称。
起始日期：	显示节假日起始日期。
终止日期：	显示节假日终止日期。

10.2 ACL配置

在 ACL 功能中，一个 ACL 可以包括多个规则，而每个规则可以针对数据包中特定字段内容进行匹配。在报文匹配规则时，会按照匹配顺序去匹配定义的规则，一旦有一条规则被匹配，报文就不再继续匹配其它规则了，交换机将对该报文执行第一次匹配的规则指定的动作，以此来提高交换机的效率。

ACL 配置功能包括 **ACL 列表**、**新建 ACL**、**MAC ACL**、**标准 IP ACL** 和**扩展 IP ACL** 五个配置页面。

10.2.1 显示ACL

在 ACL 列表页面，可以查看交换机中当前已配置的 ACL 详细信息。

进入页面的方法：访问控制>>ACL 配置>>ACL 列表



图10-4 查看 ACL 列表

条目介绍：

➢ **ACL 显示**

选择 ACL： 选择已创建的 ACL。

ACL 类型： 显示该 ACL 的类型。

规则排序： 显示该 ACL 内部的规则如何排序。

➢ 规则列表

此处可以查看或编辑 ACL 内部的详细规则信息，点击条目的操作按键可以对规则条目进行排序。

10.2.2 新建ACL

在新建 ACL 页面，可以创建 ACL。

进入页面的方法：访问控制>>ACL 配置>>新建 ACL

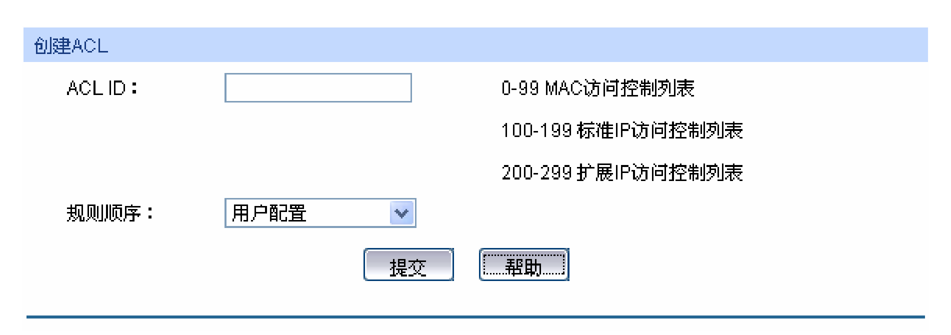


图10-5 创建 ACL

条目介绍：

➢ 创建 ACL

ACL ID： 配置 ACL ID。

规则排序： 配置该 ACL 内部的规则如何排序。默认为用户配置。
用户配置：按照用户配置规则的先后顺序进行规则匹配。

10.2.3 MAC ACL

MAC ACL 根据数据包的源 MAC 地址、目的 MAC 地址、VLAN、二层协议类型等二层信息制定匹

配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL 配置>>MAC ACL

MAC ACL
访问控制列表ID： MAC访问控制列表
规则ID：
安全操作： 允许
源MAC： 地址掩码：
目的MAC： 地址掩码：
VLAN ID：
以太网类型： （4位十六进制数）
用户优先级： 无限制
时间段： 无限制
提交 帮助

图10-6 为 MAC ACL 添加规则

条目介绍：

- **MAC ACL**

访问控制列表 ID： 选择需要配置的 ACL ID。

规则 ID： 填写规则 ID。

安全操作： 选择交换机对满足匹配规则的数据包的处理方式。默认为允许。

- 允许：转发数据包。
- 丢弃：丢弃数据包。

源 MAC： 填写规则包含的源 MAC 地址信息。

目的 MAC： 填写规则包含的目的 MAC 地址信息。

地址掩码： 填写 MAC 地址掩码，掩码置 1 表示严格匹配。

VLAN ID： 配置规则包含的 VLAN 信息。

以太网类型： 配置规则包含的以太网类型信息。

用户优先级： 选择该规则对数据包的 tag 优先级字段的匹配要求。默认为无限制。

时间段： 选择规则生效的时间段名称。默认为无限制。

10.2.4 标准IP ACL

标准 IP ACL 可以根据数据包的 IP 地址信息制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL 配置>>标准 IP ACL

标准IP ACL

访问控制列表ID： 标准IP访问控制列表

规则ID：

安全操作： 允许

分片报文：

源IP： 地址掩码：

目的IP： 地址掩码：

时间段： 无限制

提交 帮助

图10-7 为标准 IP ACL 添加规则

条目介绍：

➢ **标准 IP ACL**

访问控制列表 ID： 选择需要配置的 ACL ID。

规则 ID： 填写规则 ID。

安全操作： 选择交换机对满足匹配规则的数据包的处理方式。默认为允许。

- 允许：转发数据包。
- 丢弃：丢弃数据包。

分片报文： 选择此规则是否对分片报文生效。当选择支持分片报文时，此规则对所有分片报文进行处理，而最后一片报文总是允许转发。

源 IP： 填写规则包含的源 IP 地址信息。

目的 IP： 填写规则包含的目的 IP 地址信息。

地址掩码： 填写 IP 地址掩码，掩码置 1 表示严格匹配。

时间段： 选择规则生效的时间段名称。

10.2.5 扩展IP ACL

扩展 IP ACL 可以根据报文的源 IP 地址信息、目的 IP 地址信息、IP 承载的协议类型、协议的特性等信息来制定匹配规则，对数据包进行相应的分析处理。

进入页面的方法：访问控制>>ACL 配置>扩展 IP ACL

扩展IP ACL

访问控制列表ID： 扩展IP访问控制列表
规则ID：
安全操作： 允许
分片报文：
源IP： 地址掩码：
目的IP： 地址掩码：
IP 协议： 无限制
选择ICMP： 无限制
ICMP类型： ICMP代码：
TCP Flag： URG * ACK * PSH * RST * SYN * FIN *
源端口号：
目的端口号：
DSCP： 无限制
IP ToS： 无限制 IP Pre： 无限制
时间段： 无限制
提交 帮助

图10-8 为扩展 IP ACL 添加规则

条目介绍：

➢ **扩展 IP ACL**

访问控制列表 ID：	选择需要配置的 ACL ID。
规则 ID：	填写规则 ID。
安全操作：	选择交换机对满足匹配规则的数据包的处理方式。默认为允许。 ● 允许：转发数据包。 ● 丢弃：丢弃数据包。
分片报文：	选择此规则是否对分片报文生效。当选择支持分片报文时，此规则对所有分片报文进行处理，而最后一片报文总是允许转发。
源 IP：	填写规则包含的源 IP 地址信息。
目的 IP：	填写规则包含的目的 IP 地址信息。
地址掩码：	填写 IP 地址掩码，掩码置 1 表示严格匹配。
IP 协议：	选择规则包含的 IP 协议信息。
选择 ICMP：	当 IP 协议选择 ICMP 时，此处配置预定义的 ICMP 类型和代码。
ICMP 类型：	配置自定义的 ICMP 名称。
ICMP 代码：	配置自定义的 ICMP 代码。
TCP Flag：	当 IP 协议选择 TCP 时，此处配置 Flag 匹配条件。

源端口号： 当 IP 协议选择 TCP/UDP 时，此处配置规则包含的 TCP/UDP 源端口号。

目的端口号： 当 IP 协议选择 TCP/UDP 时，此处配置规则包含的 TCP/UDP 目的端口号。

DSCP： 填写规则包含的 DSCP 域信息。

IP ToS： 填写规则包含的 IP ToS 字段信息。

IP Pre： 填写规则包含的 IP Precedence 字段信息。

时间段： 选择规则生效的时间段名称。

10.3 Policy配置

Policy 功能是将 ACL 规则和处理方式组合起来，组成一个访问控制策略，对符合相应 ACL 规则的数据包进行控制，处理方式包括流镜像、流监控、QoS 重标记和端口重定向。

Policy 配置功能包括**显示 Policy**、**新建 Policy**、**配置 Policy** 三个配置页面。

10.3.1 显示Policy

在 Policy 页面可以查看和编辑 ACL 规则的数据包处理方式，此动作是对匹配了相应 ACL 规则的数据包的处理方式。

进入页面的方法：访问控制>>Policy 配置>显示 Policy



图10-9 查看 Policy 列表

条目介绍：

➢ **Policy 显示**

选择 Policy： 选择需要查看的 policy 名称。当需要删除相应的 policy 时，选择后点击删除按键即可。

➢ **Action 列表**

选择： 选择动作条目进行删除。

序号： 显示动作条目的序号。

ACL ID： 显示此 Policy 中包含的 ACL。

流镜像： 显示此 Policy 中的流镜像端口。

流监管： 显示该 Policy 中添加的流监管动作信息。

端口重定向： 显示该 Policy 中添加的端口重定向动作信息。

QoS 重标记： 显示该 Policy 中添加的 QoS 重标记动作信息。

操作： 点击<编辑>按键，可以对编辑相应的 policy 条目。

10.3.2 新建Policy

在此页面中可以创建 Policy。

进入页面的方法：访问控制>>Policy 配置>新建 Policy

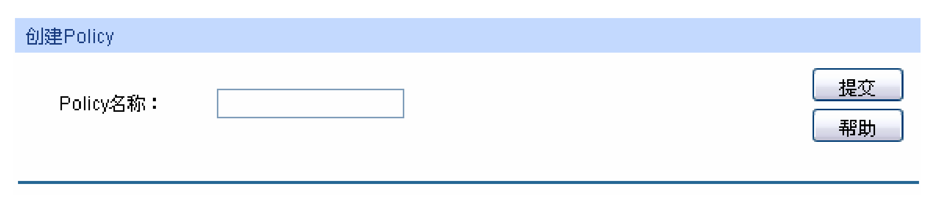


图10-10 创建 Policy

条目介绍：

➢ **创建 Policy**

Policy 名称： 填写 Policy 的名称。

10.3.3 配置Policy

在此页面中，可以配置 Policy 对应的 ACL 规则以及包含的动作，此动作是对匹配了相应 ACL 规则的数据包的处理方式。

进入页面的方法：访问控制>>Policy 配置>Policy 设置

Policy设置：

选择Policy： 选择Policy名称

选择ACL： 选择ACL

☐ 流镜像

镜像端口： Port 1

☐ 流监管

额定速率： Kbps(1-1000000)

超速处理： 不处理

☐ 端口重定向

指定出口端口： 所有端口

指定VID：

☐ QoS重标记

DSCP： 无限制

本地优先级： 默认

提交 帮助

图10-11 为 Policy 添加 ACL 并设置动作

条目介绍：

➢ **Policy 设置**

选择 Policy： 选择 Policy 的名称。

选择 ACL： 选择 ACL 作为 Policy 作用的对象。

流镜像： 配置该 Policy 的数据包执行流镜像动作，镜像到选定的端口。

流监管： 配置该 Policy 的数据包执行流限速动作。

- 额定速率：为匹配了相应 ACL 的数据包配置额定转发速率。
- 超速处理：为超过额定速率的数据包选择处理方式。

端口重定向： 配置该 Policy 的数据包执行端口重定向动作，改变转发端口。

- 指定出口端口：将匹配了相应 ACL 规则的数据包指定转发端口。
- 指定 VID：将匹配了相应 ACL 规则的数据包指定转发 VLAN。

QoS 重标记： 配置该 Policy 的数据包执行 QoS 动作，根据 QoS 功能具体配置情况转发。

- DSCP：为匹配了相应 ACL 的数据包指定 DSCP 域。
- 本地优先级：为匹配了相应 ACL 的数据包指定优先级。

10.4 绑定配置

只有将 Policy 和端口/VLAN 绑定，Policy 才能生效；将 Policy 与端口/VLAN 进行绑定后，端口和 VLAN 会对接收到的数据包根据 Policy 进行匹配处理。绑定配置功能将 Policy 应用到某个端口或者 VLAN 上。

绑定配置功能包括**显示绑定**、**端口绑定**、**VLAN 绑定**三个配置页面。

10.4.1 显示绑定

在此页面中可以查看已进行端口/VLAN 绑定的 Policy 条目。

进入页面的方法：访问控制>>绑定配置>显示绑定



图10-12 查看 Policy 与端口/VLAN 绑定信息

条目介绍：

➢ 选择显示模式

选择显示模式：	请根据需要选择参考已绑定的条目类别。

➢ **Policy** 绑定列表

选择：	选择绑定条目进行删除。
序号：	显示绑定条目的序号。
Policy 名称：	显示绑定的 Policy 名称。
绑定接口：	显示与相应 Policy 绑定的端口号或 VID。
方向：	显示绑定的方向。本交换机当前仅支持入口方向的过滤。

10.4.2 端口绑定

在此页面中可以将 Policy 与端口进行绑定。

进入页面的方法：访问控制>>绑定配置>端口绑定



图10-13 将 Policy 与端口进行绑定

条目介绍：

➢ 端口绑定配置

Policy 名称：	选择需要绑定的 Policy 名称。

端口： 配置需要绑定的端口号。

➢ 端口绑定列表

序号： 显示绑定条目的序号。

Policy 名称： 显示绑定的 Policy 名称。

端口： 显示与相应 Policy 绑定的端口号。

方向： 显示绑定的方向。本交换机当前仅支持入口方向的过滤。

10.4.3 VLAN绑定

在此页面中可以将 Policy 与 VLAN 进行绑定。

进入页面的方法：访问控制>>绑定配置>VLAN 绑定



图10-14 将 Policy 与 VLAN 进行绑定

条目介绍：

➢ **VLAN 绑定配置**

Policy 名称： 选择需要绑定的 Policy 名称。

VLAN ID： 填写需要绑定的已建立的 VLAN ID。

➢ **VLAN 绑定列表**

序号： 显示绑定条目的序号。

Policy 名称： 显示绑定的 Policy 名称。

VLAN ID： 显示与相应 Policy 绑定的 VLAN ID。

方向： 显示绑定的方向。本交换机当前仅支持入口方向的过滤。

配置步骤：

步骤	操作	说明
1	设置生效时间段	必选操作。在**访问控制>>时间段配置**三个标签页中配置 ACL 规则的生效时间段。
2	配置 ACL 规则	必选操作。在**访问控制>>ACL 配置**三个标签页中配置 ACL 规则对数据包进行匹配。

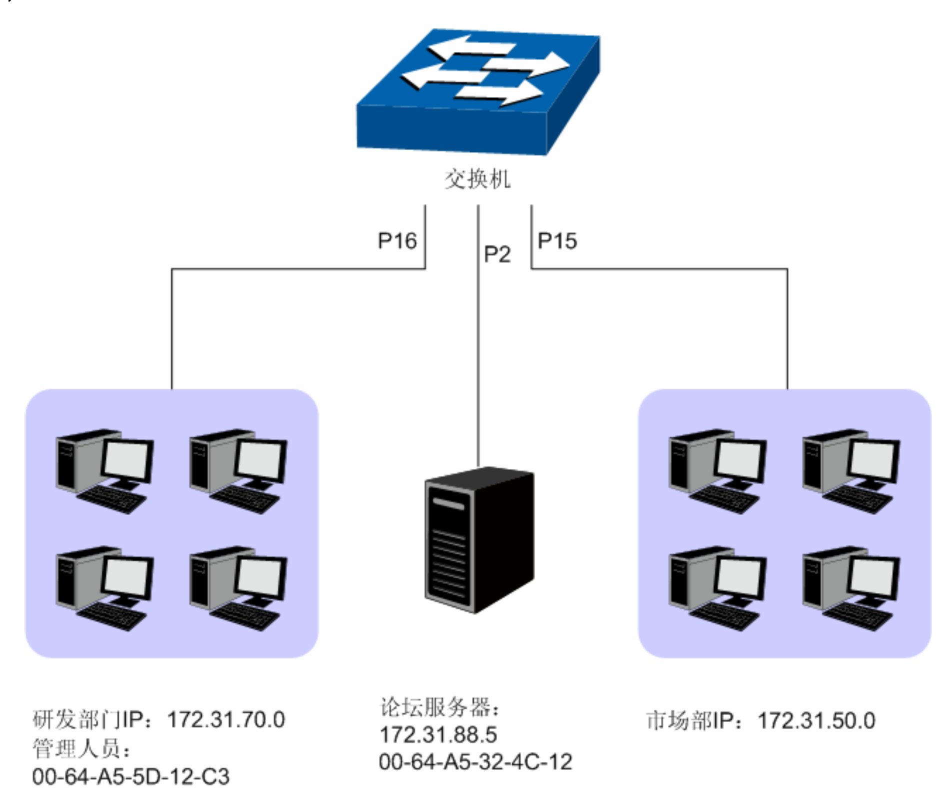
3	配置 Policy	必选操作。在**访问控制>>Policy 配置**三个标签页中配置 Policy，对匹配了相应 ACL 规则的数据包，可以通过 Policy 设置处理方式。
4	将 Policy 与端口/VLAN 绑定	必选操作。在**访问控制>>绑定配置**三个标签页中将 Policy 与端口/VLAN 进行绑定，将 Policy 应用到相应的端口/VLAN 上。

10.5 访问控制功能组网应用

➢ 组网需求

1. 研发部门的管理人员自由访问公司论坛以及上网，管理人员 MAC 地址为 00-46-A5-5D-12-C3。
2. 研发部门工作人员在工作时间不可以上网，全天访问公司论坛。
3. 市场部人员可以全天候上网，工作时间不能访问公司论坛。
4. 市场部和研发部门之间互相不能访问。

➢ 组网图



➢ 配置步骤

步骤	操作	说明
1	配置时间段	在**访问控制>>时间段配置**功能处，新建时间段，描述为 work_time，时间段采用周期时间，周期时间选择工作日周一到周五，时间片段添加 08:00~18:00。

2	需求 1 配置	在**访问控制>>ACL 配置>>新建 ACL** 页面，创建 ACL 11。 在**访问控制>>ACL 配置>>MAC ACL** 页面，选择 ACL 11，创建规则 1，安全操作设置为允许；勾选源 MAC 设置为 00-46-A5-5D-12-C3，掩码为 FF-FF-FF-FF-FF-FF；时间段选择无限制。 在**访问控制>>Policy 配置>>新建 Policy** 页面，创建 Policy，名称定为 manager。 在**访问控制>>Policy 配置>>配置 Policy** 页面，将 ACL 11 应用到 Policy manager。 在**访问控制>>Policy 配置>>端口绑定**页面，选择 Policy manager 与端口 16 绑定。
3	需求 2、4 配置	在**访问控制>>ACL 配置>>新建 ACL** 页面，创建 ACL 100。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 100，创建规则 1，安全操作设置为禁止；设置源 IP 为 172.31.70.1，掩码为 255.255.255.0；设置目的 IP 为 172.31.50.1，掩码为 255.255.255.0；时间段选择无限制。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 100，创建规则 2，安全操作设置为允许；设置源 IP 为 172.31.70.1，掩码为 255.255.255.0；设置目的 IP 为 172.31.88.5，掩码为 255.255.255.255；时间段选择无限制。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 100，创建规则 3，安全操作设置为禁止；设置源 IP 为 172.31.70.1，掩码为 255.255.255.0；时间段选择 work_time。 在**访问控制>>Policy 配置>>新建 Policy** 页面，创建 Policy，名称定为 limit1。 在**访问控制>>Policy 配置>>配置 Policy** 页面，将 ACL 100 应用到 Policy limit1。 在**访问控制>>Policy 配置>>端口绑定**页面，选择 Policy limit1 与端口 16 绑定。

4	需求 3、4 配置	在**访问控制>>ACL 配置>>新建 ACL** 页面，创建 ACL 101。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 101，创建规则 1，安全操作设置为禁止；设置源 IP 为 172.31.50.1，掩码为 255.255.255.0；设置目的 IP 为 172.31.88.5，掩码为 255.255.255.255；时间段选择 work_time。 在**访问控制>>ACL 配置>>标准 IP ACL** 页面，选择 ACL 101，创建规则 2，安全操作设置为禁止；设置源 IP 为 172.31.50.1，掩码为 255.255.255.0；设置目的 IP 为 172.31.70.1，掩码为 255.255.255.0；时间段选择无限制。 在**访问控制>>Policy 配置>>新建 Policy** 页面，创建 Policy，名称定为 limit2。 在**访问控制>>Policy 配置>>配置 Policy** 页面，将 ACL 101 应用到 Policy limit2。 在**访问控制>>Policy 配置>>端口绑定**页面，选择 Policy limit2 与端口 18 绑定。

回目录

第11章 网络安全

网络安全模块为保护局域网安全提供了多项安全措施，包括**四元绑定**、**ARP 防护**、**IP 源防护**、**DoS 防护**以及 **802.1X 认证**五个部分，请根据实际需要进行配置。

11.1 四元绑定

四元绑定，是将计算机的 MAC 地址、IP 地址、所属 VLAN 以及与之相连的交换机的端口号四者绑定，以下这四个参数信息简称四元信息。该功能可以启用 ARP 防护和 IP 源防护，只有符合绑定关系的计算机才能访问网络。

本交换机支持如下三种四元绑定方式：

1) 手动绑定，通过手动方式绑定局域网用户的四元信息。当可以全面获取正确的局域网用户的四元信息时，可通过此方式进行绑定。

2) 扫描绑定：通过 ARP 扫描获取局域网用户的四元信息，并根据实际需要选择扫描结果进行绑定。此绑定方式只需在相应的功能页面输入 IP 地址段进行扫描。

3) DHCP 侦听：通过 DHCP 侦听功能侦听 DHCP 广播包，记录数据包中的 IP、MAC 和 VLAN ID 等信息。当局域网中搭建了 DHCP 服务器给局域网用户分配 IP 地址时，DHCP 侦听功能可以很方便地记录局域网用户的四元信息。

此三种方式也称为四元绑定条目的三个来源。三种来源的四元绑定条目信息必须完全不一致，以避免冲突。如果四元绑定条目发生冲突，只有“来源”优先级最高的条目生效。此三种来源方式中，手动绑定优先级最高，其次是扫描绑定，DHCP 侦听优先级最低。

本功能包括**绑定列表**、**手动绑定**、**扫描绑定**和 **DHCP 侦听**四个配置页面。

11.1.1 绑定列表

在绑定列表页面中，可以查看当前交换机已进行四元绑定的局域网计算机条目信息。

进入页面的方法：网络安全>>四元绑定>>绑定列表



图11-1 查看四元绑定信息

条目介绍：

➢ 来源筛选

来源：	选择查看不同来源的四元绑定条目。 ● 全部来源：查看全部四元绑定条目。 ● 手动添加：只查看手动添加的四元绑定条目。 ● ARP 扫描：只查看通过 ARP 扫描获得的四元绑定条目。 ● DHCP 侦听：只查看通过 DHCP 侦听获得的四元绑定条目。

➢ 四元绑定表

IP 选择：	点击<选择>按键，可根据所输 IP 快速查找四元绑定条目。
选择：	勾选条目可修改主机名及防护范围，可多选。
主机名：	显示主机描述名称。
IP 地址：	显示主机 IP 地址。
MAC 地址：	显示主机 MAC 地址。
VLAN ID：	显示 VLAN ID。
端口：	显示主机连接的交换机端口。
防护范围：	显示并编辑此条目支持的防护范围。
来源：	显示此条目的来源。
冲突：	显示此绑定条目与其它条目的冲突状态。 ● 警告：表示此条目冲突可能是由于 MSTP 等功能造成的。 ● 严重：已确定的冲突条目。

注意：

- 冲突等级为“严重”的条目只有“来源”优先级最高的一条生效。
- 多条“来源”优先级相同的条目中只有最后添加/修改的条目生效。

11.1.2 手动绑定

当已经获取了局域网用户的四元信息时，可以将四元信息静态绑定。

进入页面的方法：网络安全>>四元绑定>>手动绑定

手动绑定

主机名： （长度限制为20字符）

IP地址： （格式为：192.168.0.1）

MAC地址： （格式为：00-00-00-00-00-01）

VLAN ID： （1-4094）

端口： 1

防护范围： 不启用

绑定

手动绑定条目

选择	主机名	IP地址	MAC地址	VLAN ID	端口	防护范围	冲突

全选 删除 帮助

当前条目总数：0

注意：

1、冲突等级为"严重"的条目只有"来源"优先级最高的一条生效。

2、多条"来源"优先级相同的条目中只有最后添加/修改的条目生效。

图11-2 手动绑定四元信息

条目介绍：

➢ 手动绑定

主机名： 输入主机描述名称。

IP 地址： 输入主机 IP 地址。

MAC 地址： 输入主机 MAC 地址。

VLAN ID： 输入 VLAN ID。

端口： 输入主机连接的交换机端口。

防护范围： 选择此条目支持的防护范围。

绑定： 点击此按键将上述输入信息进行绑定。

➢ 手动绑定条目

选择： 勾选条目进行删除。

主机名： 显示主机描述名称。

IP 地址： 显示主机 IP 地址。

MAC 地址： 显示主机 MAC 地址。

VLAN ID： 显示 VLAN ID。

端口： 显示主机连接的交换机端口。

防护范围： 显示此条目支持的防护范围。

冲突： 显示此绑定条目与其它条目的冲突状态。

- 警告：表示此条目冲突可能是由于 MSTP 等功能造成的。
- 严重：已确定的冲突条目。

11.1.3 扫描绑定

ARP（Address Resolution Protocol，地址解析协议）用于将网络层的 IP 地址解析为数据链路层地址。IP 地址只是主机在网络层中的地址，如果要将网络层中数据包传送给目的主机，必须知道目的主机的数据链路层地址（比如以太网络 MAC 地址）。因此必须将 IP 地址解析为数据链路层地址。

ARP协议用于将IP地址解析为MAC地址，并在主机内部维护一张ARP表，记录最近与本主机通信的其它主机的MAC地址与IP地址的对应关系。当主机需要与陌生主机通信时，首先进行ARP地址解析，ARP地址解析过程如图11-3所示：

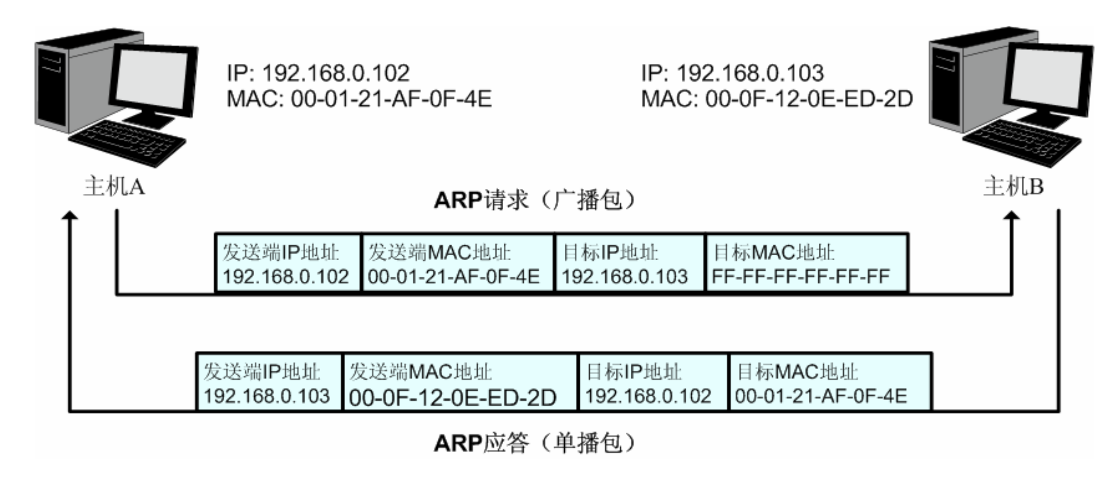


图11-3 ARP 地址解析图

1) A 在自己的 ARP 表中查询是否存在主机 B 的 IP 地址和 MAC 地址的对应条目。若存在，直接向主机 B 发送数据。若不存在，则 A 向整个局域网中广播一份称为“ARP 请求”的数据链路帧，这个请求包含发送端（即主机 A）的 IP 地址和 MAC 地址以及接收端（即主机 B）的 IP 地址。
2) 局域网的每个主机接收到主机 A 广播的 ARP 请求后，目的主机 B 识别出这是发送端在询问它的 IP 地址，于是给主机 A 发出一个 ARP 应答。这个应答包含了主机 B 的 MAC 地址。
3) 主机 A 接收到主机 B 发出的 ARP 应答后，就将主机 B 的 IP 地址与 MAC 地址的对应条目添加自己的 ARP 表中，以便后续报文的转发。

扫描绑定功能即通过交换机向局域网或 VLAN 发送指定 IP 段的 ARP 请求报文，当收到相应的 ARP 应答报文时，将分析 ARP 应答报文来获得四元信息。由此可见，通过扫描绑定功能可以很方便的将局域网用户的四元信息进行绑定。

进入页面的方法：网络安全>>四元绑定>>扫描绑定

ARP扫描

起始IP地址：

结束IP地址： 扫描

VLAN ID： （1 - 4094）

扫描结果

选择	主机名	IP地址	MAC地址	VLAN ID	端口	防护范围	冲突
□							

绑定 删除 帮助

当前条目总数：0

注意：

1、VLAN ID选项适用于扫描存在跨交换机VLAN的网络拓扑

2、VLAN ID选项用于指定ARP扫描所使用的报文所带的VLAN Tag，且不受交换机VLAN配置的限制

3、当VLAN ID为空时交换机会使用不带VLAN TAG的数据包进行扫描

图11-4 扫描绑定四元信息

条目介绍：

➢ **ARP 扫描**

起始 IP 地址： 输入起始 IP 地址。

结束 IP 地址： 输入结束 IP 地址。

VLAN ID: 输入 VLAN ID，在相应的 VLAN 中进行扫描。若留空，则发送 untag 数据包进行扫描。

扫描： 点击<扫描>按键将对局域网计算机进行扫描。

➢ 扫描结果

选择： 勾选条目进行绑定或删除。

主机名： 显示主机描述名称或对主机进行描述以便区分。

IP 地址： 显示主机 IP 地址。

MAC 地址： 显示主机 MAC 地址。

VLAN ID： 显示 VLAN ID。

端口： 显示主机连接的交换机端口。

防护范围： 显示此条目支持的防护范围或者对此条目开启防护功能。

冲突： 显示此绑定条目与其它条目的冲突状态。

- 警告：表示此条目冲突可能是由于 MSTP 等功能造成的。
- 严重：已确定的冲突条目。

11.1.4 DHCP侦听

随着网络规模的不断扩大和网络复杂度的提高，经常出现计算机的数量超过可供分配的 IP 地址的情况。同时随着便携机及无线网络的广泛使用，计算机的位置也经常变化，相应的 IP 地址也必须经常更新，从而导致网络配置越来越复杂。DHCP（Dynamic Host Configuration Protocol，动态主机配

置协议）是在 BOOTP 协议基础上进行了优化和扩展而产生的一种网络配置协议，并有效解决了上面这些问题。

➢ **DHCP 工作原理**

DHCP采用“客户端/服务器”通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的IP地址等配置信息，以实现网络资源的动态配置。通常一台服务器可以为多台客户端分配IP，如图11-5所示：

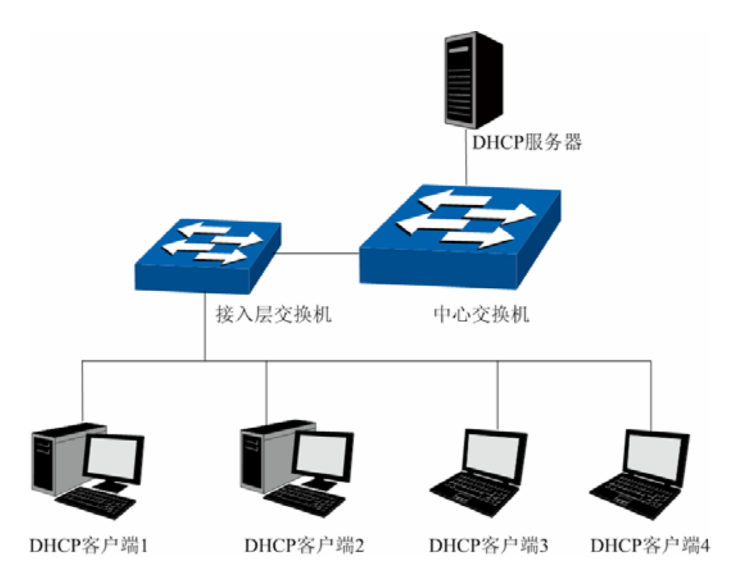


图11-5 DHCP 网络典型应用

针对 DHCP 客户端的需求不同，DHCP 服务器提供三种 IP 地址分配策略：

1) 手工分配地址：由管理员为少数特定客户端（如 WWW 服务器等）静态绑定 IP 地址。通过 DHCP 将固定 IP 地址分配给客户端。
2) 自动分配地址：DHCP 服务器为客户端分配租期为无限长的 IP 地址。
3) 动态分配地址：DHCP 服务器为客户端分配具有一定有效期限的 IP 地址，当使用期限到期后，客户端需要重新申请地址。

绝大多数客户端均通过动态分配地址的方式获取 IP 地址，其获取 IP 地址的过程如下图所示：

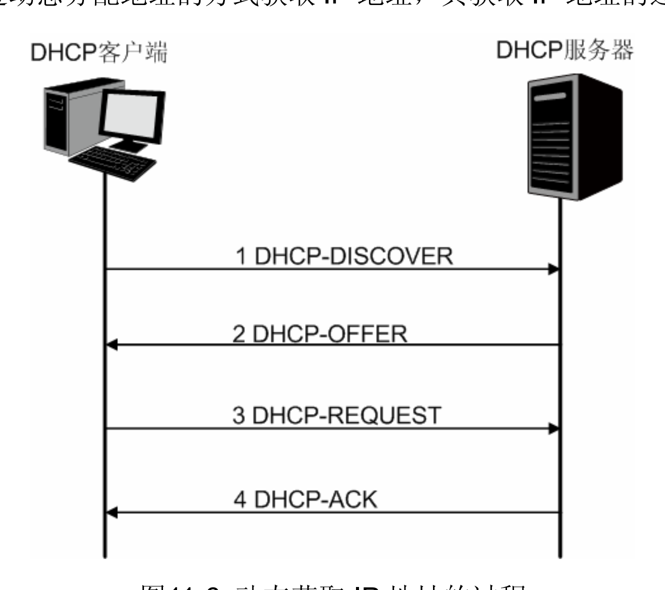


图11-6 动态获取 IP 地址的过程

1) 发现阶段，客户端以广播方式发送 DHCP-DISCOVER 报文寻找 DHCP 服务器。

2) 提供阶段，DHCP 服务器接收到客户端发送的 DHCP-DISCOVER 报文后，根据 IP 地址分配的优先次序从地址池中选出一个 IP 地址，与其它参数一起通过 DHCP-OFFER 报文发送给客户端（发送方式根据客户端发送的 DHCP-DISCOVER 报文中的 flag 字段决定，具体请见 DHCP 报文格式的介绍）。

3) 选择阶段，如果有多台 DHCP 服务器向该客户端发来 DHCP-OFFER 报文，客户端只接受第一个收到的 DHCP-OFFER 报文，然后以广播方式发送 DHCP-REQUEST 报文，该报文中包含 DHCP 服务器在 DHCP-OFFER 报文中分配的 IP 地址。

4) 确认阶段，DHCP 服务器收到 DHCP 客户端发来的 DHCP-REQUEST 报文后，只有 DHCP 客户端选择的服务器会进行如下操作：如果确认地址分配给该客户端，则返回 DHCP-ACK 报文；否则将返回 DHCP-NAK 报文，表明地址不能分配给该客户端。

➢ **Option 82**

DHCP 报文格式基于 BOOTP 的报文格式，共有 8 种类型的报文，每种报文的格式相同。DHCP 和 BOOTP 消息的不同主要体现在选项（Option）字段，并利用 Option 字段来实现功能扩展。例如 DHCP 可以利用 Option 字段传递控制信息和网络配置参数，实现地址的动态分配，为客户端提供更加丰富的网络配置信息。更多 DHCP Option 选项的介绍，请参见 RFC 2132。

Option 82 选项记录了 DHCP 客户端的位置信息，交换机接收到 DHCP 客户端发送给 DHCP 服务器的请求报文后，在该报文中添加 Option 82，并转发给 DHCP 服务器。管理员可以从 Option 82 中获得 DHCP 客户端的位置信息，以便定位 DHCP 客户端，实现对客户端的安全和计费等控制。支持 Option 82 的服务器还可以根据该选项的信息制订 IP 地址和其它参数的分配策略，提供更加灵活的地址分配方案。

Option 82 最多可以包含 255 个子选项。若定义了 Option 82，则至少要定义一个子选项。目前本交换机支持两个子选项：Circuit ID（电路 ID 子选项）和 Remote ID（远程 ID 子选项）。由于 Option 82 的内容没有统一规定，不同厂商通常根据需要进行填充。目前本交换机对子选项的填充内容如下，电路 ID 子选项的填充内容是接收到 DHCP 客户端请求报文的端口所属 VLAN 的编号以及端口号，远程 ID 子选项的填充内容是接收到 DHCP 客户端请求报文的 DHCP Snooping 设备的 MAC 地址。

➢ **DHCP 服务欺骗攻击**

在 DHCP 工作过程中，通常服务器和客户端没有认证机制，如果网络上存在多台 DHCP 服务器，不仅会给网络造成混乱，也对网络安全造成很大威胁。这种网络中出现非法的 DHCP 服务器，通常分为两种情况：

1) 用户不小心配置的 DHCP 服务器，由此引起的网络混乱非常常见。

2) 黑客将正常的DHCP服务器中的IP地址耗尽，然后冒充合法的DHCP服务器，为客户端分配IP地址等配置参数。例如黑客利用冒充的DHCP服务器，为用户分配一个经过修改的DNS服务器地址，在用户毫无察觉的情况下被引导至预先配置好的假的金融网站或电子商务网站，骗取用户的帐户和密码，如图11-7所示。

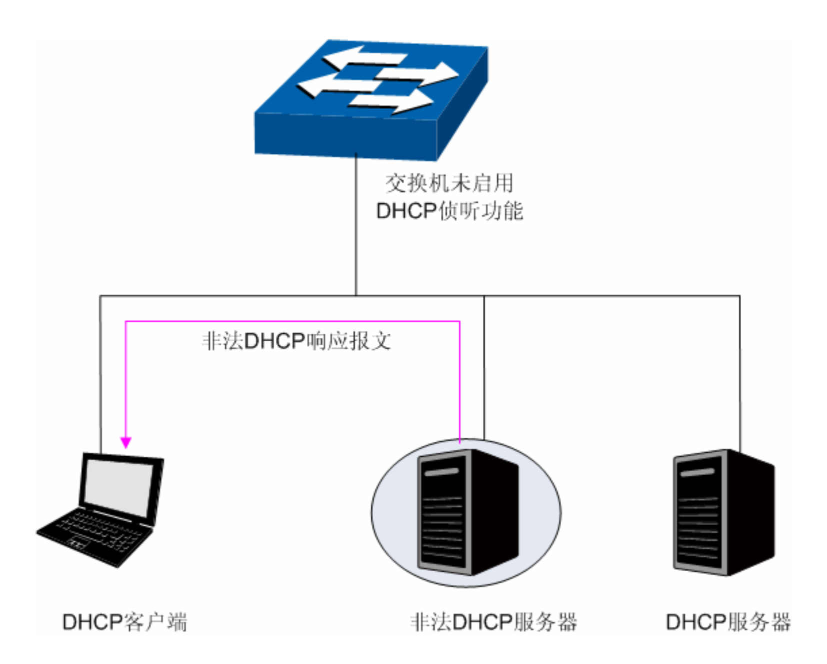


图11-7 DHCP 服务欺骗攻击

DHCP 侦听是运行在交换机上的一种 DHCP 安全特性。通过设置 DHCP 服务器的连接端口为授信端口，只处理授信端口发来的 DHCP 响应报文；通过监听 DHCP 报文，记录用户从 DHCP 服务器获取局域网用户的四元信息，进行绑定后与 ARP 攻击防护、IP 源防护等安全功能配合使用；同时也可以过滤不可信任的 DHCP 信息，防止局域网中发生 DHCP 服务欺骗攻击，提高网络的安全性。

进入页面的方法：网络安全>>四元绑定>>DHCP 侦听



图11-8 DHCP 侦听

注意：

- 若 LAG 组成员端口需要配置 DHCP 侦听功能，请保持端口的参数一致。

条目介绍：

➢ **DHCP 侦听配置**

DHCP 侦听： 选择是否启用 DHCP 侦听功能。默认未启用。

全局流量控制： 填写交换机每秒允许转发的 DHCP 消息的数目，超出的部分将被丢弃。

Decline 保护阀值： 选择触发特定端口 Decline 保护所需的 Decline 报文最小流量。

Decline 保护流量限制： 如果端口 Decline 消息流量超出阈值，则将相应端口的端口流量限制设置为该值。

➢ **Option 82 配置**

Option 82 功能： 选择是否启用 Option 82 字段。默认未启用。

已有 Option 82 字段： 当客户端的 DHCP 请求报文已经有 Option 82 字段时，选择对此字段的操作。

- 保留：保留数据包中的 Option 字段信息。
- 替换：替换数据包中的 Option 字段信息，替换为交换机自定义的系统选项内容。
- 丢弃：丢弃包含 Option 82 字段的数据包。

自定义选项内容： 选择交换机是否自定义 Option 82 选项内容。

电路 ID 子选项： 输入交换机自定义的 Option 82 选项中电路 ID 子选项的内容。

远程 ID 子选项： 输入交换机自定义的 Option 82 选项中远程 ID 子选项的内容。

➢ 端口配置

端口选择： 点击<选择>按键，可根据所输端口号快速选择端口。

选择： 勾选端口配置端口参数，可多选。

端口： 显示交换机的端口号。

授信端口： 选择是否配置端口为授信端口，只有授信端口才正常转发来自正常 DHCP 服务器端的消息，请将连接有 DHCP 服务器的端口设为授信端口。

MAC 验证： 选择是否启用 MAC 验证功能。DHCP 消息中有两个字段存储着客户端的 MAC 地址，MAC 验证功能会对这两个字段进行比较，如果不同，则将消息丢弃。

流量控制： 选择是否对 DHCP 数据包启用流量控制功能，超出流量部分的 DHCP 数据包将被丢弃。

Decline 侦听： 选择是否启用端口的 Decline 侦听功能。

LAG： 显示端口当前所属的汇聚组。

11.2 ARP防护

根据11.1.3 扫描绑定所述的ARP地址解析过程可知，利用ARP协议，可以实现相同网段内的主机之间正常通信或者通过网关与外网进行通信。但由于ARP协议是基于网络中的所有主机或者网关都为可信任的前提制定的，因此在实际复杂的网络中，此过程存在大量的安全隐患，从而导致针对ARP协议的欺骗攻击非常常见。网关仿冒、欺骗网关、欺骗终端用户和ARP泛洪攻击均是在学校等大型网络中常见的ARP攻击，以下简单介绍这几种常见攻击：

➢ 网关仿冒

攻击者发送错误的网关MAC给受害者，而网络中的受害者收到这些ARP响应报文时，自动更新ARP表，导致不能正常访问网络。如图11-9所示。

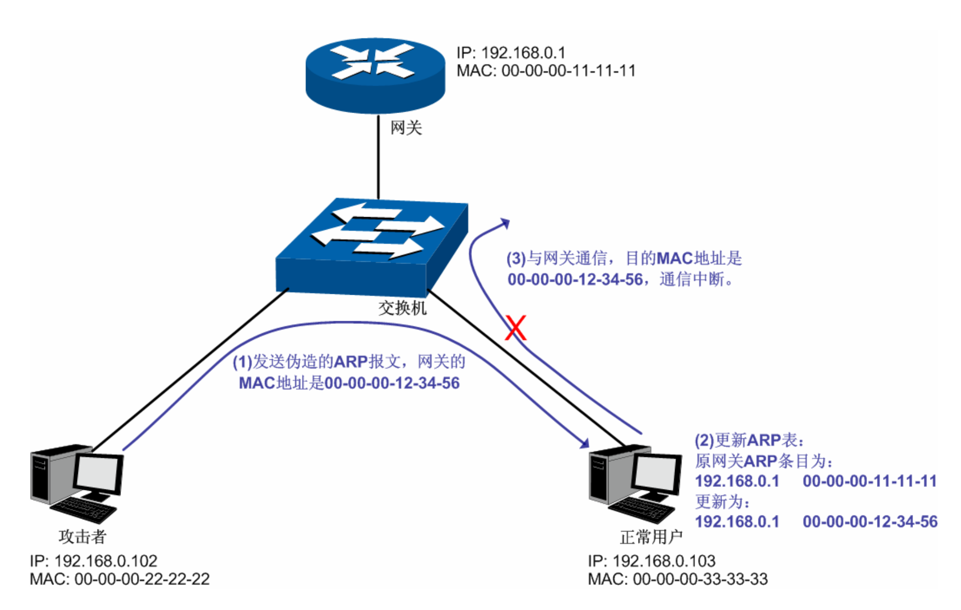


图11-9 ARP 攻击-网关仿冒示意图

如图，攻击者发送伪造的网关 ARP 报文给局域网中的正常用户，相应的局域网用户收到此报文后更新自己的 ARP 表项。当局域网中正常用户要与网关进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

➢ 欺骗网关

攻击者发送错误的终端用户的IP/MAC的对应关系给网关，导致网关无法和合法终端用户正常通信。如图11-10所示。

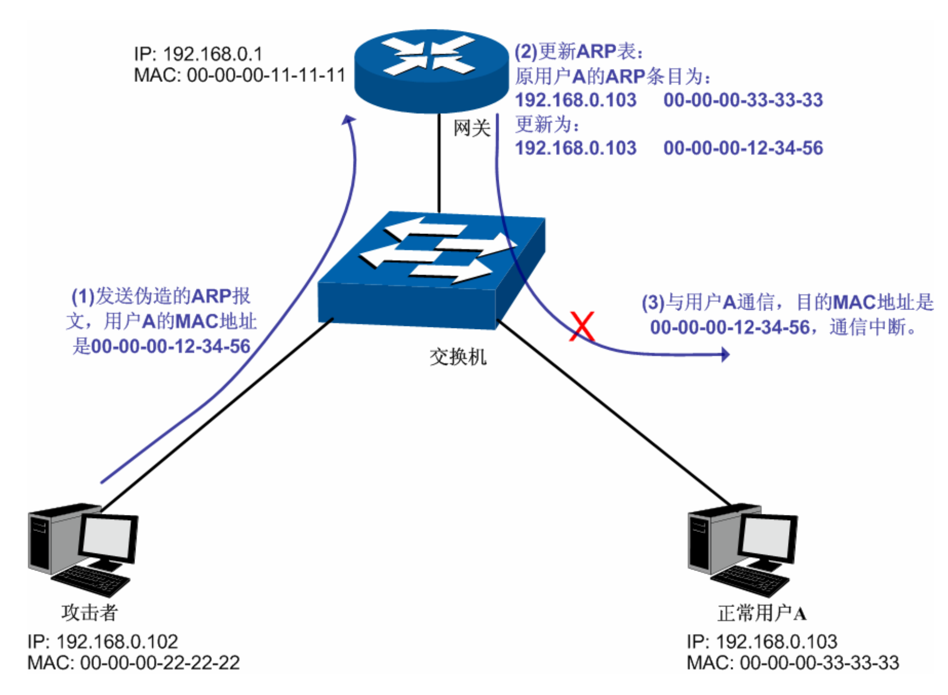


图11-10 ARP 攻击-欺骗网关示意图

如图，攻击者发送伪造的用户 A 的 ARP 报文给网关，网关收到此报文后更新自己的 ARP 表项，当网关与局域网中用户 A 进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

➢ 欺骗终端用户

攻击者发送错误的终端用户/服务器的IP/MAC的对应关系给受害的终端用户，导致同网段内两个终端用户之间无法正常通信。如图11-11所示。

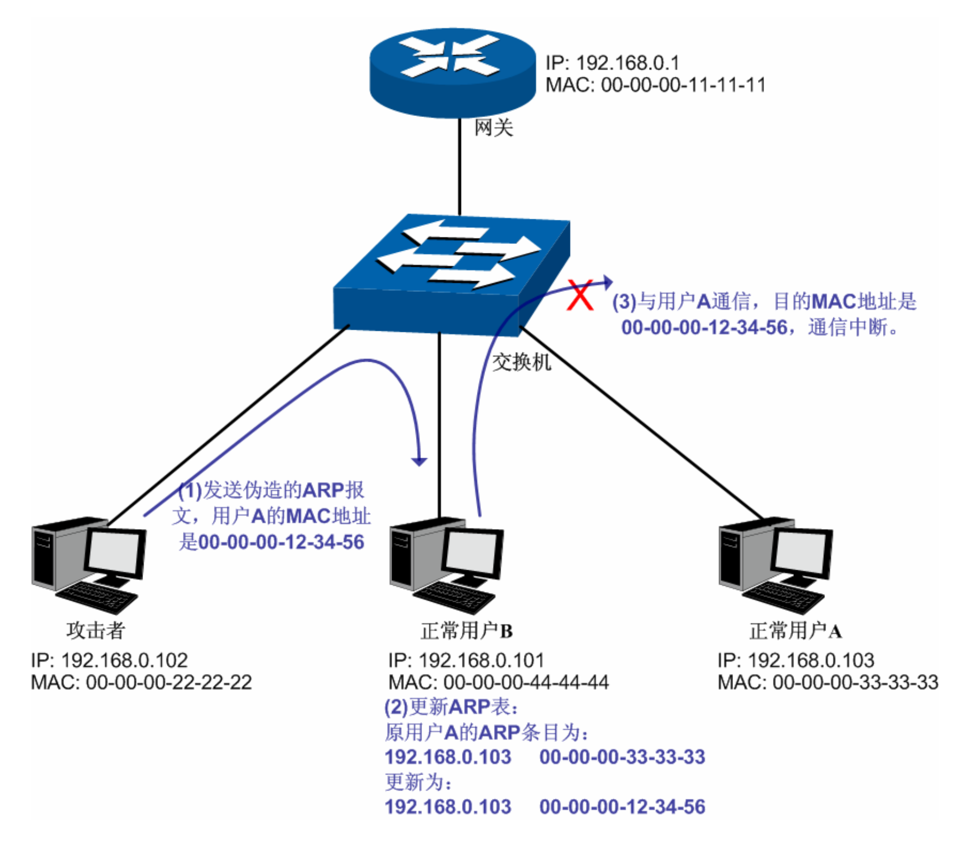


图11-11 ARP 攻击-欺骗普通用户示意图

如图，攻击者发送伪造的用户 A 的 ARP 报文给用户 B，用户 B 收到此报文后更新自己的 ARP 表项，当用户 B 与用户 A 进行通信时，将数据包封装上错误的目的 MAC 地址，导致通信中断。

- 中间人攻击

攻击者不断向局域网中计算机发送错误的ARP报文，使受害主机一直维护错误的ARP表项。当局域网主机互相通信时，将数据包发给攻击者，再由攻击者将数据包进行处理后转发。在这个过程中，攻击者窃听了通信双方的数据，而通信双方对此并不知情。这就是中间人攻击。如图11-12所示。

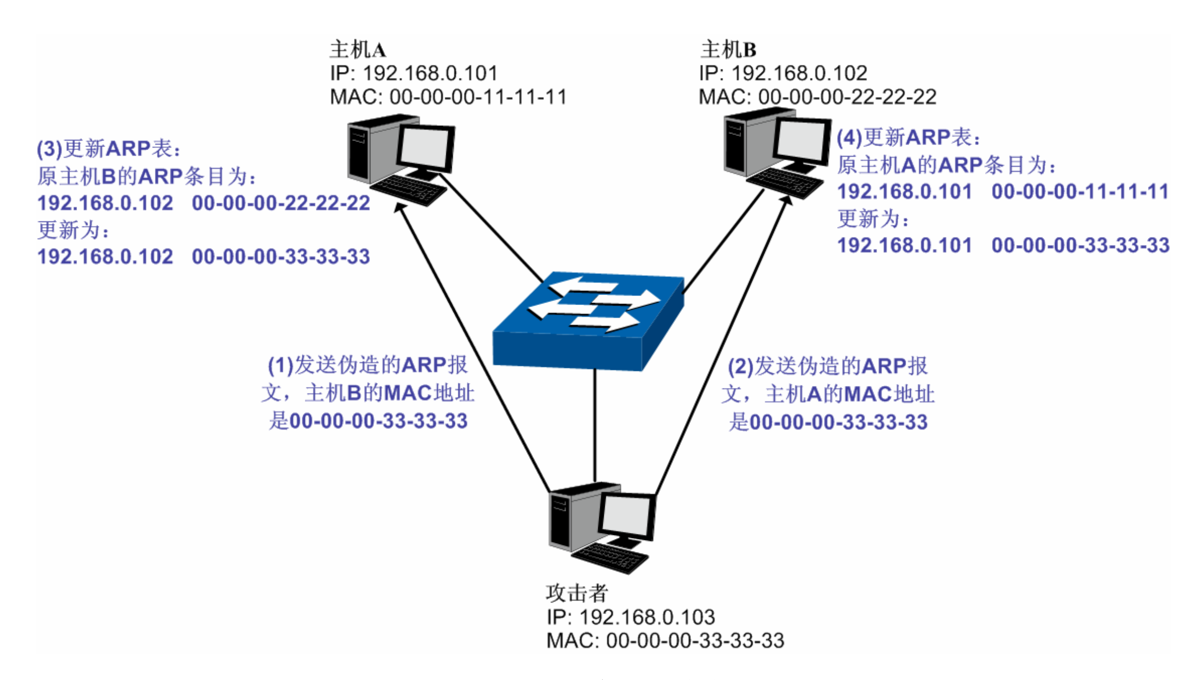


图11-12 中间人攻击

假设同一个局域网内，有 3 台主机通过交换机相连：

A 主机：IP 地址为 192.168.0.101，MAC 地址为 00-00-00-11-11-11；

B 主机：IP 地址为 192.168.0.102，MAC 地址为 00-00-00-22-22-22；

攻击者：IP 地址为 192.168.0.103，MAC 地址为 00-00-00-33-33-33。

1. 首先，攻击者向主机 A 和主机 B 发送伪造的 ARP 应答报文。
2. A 主机和 B 主机收到此 ARP 应答后，更新各自的 ARP 表。
3. A 主机和 B 主机通信时，将数据包发送给错误的 MAC 地址，即攻击者。
4. 攻击者窃听了通信数据后，将数据包处理后再转发到正确的 MAC 地址，使 A 主机和 B 主机保持正常的通信。
5. 攻击者连续不断地向 A 主机和 B 主机发送伪造的 ARP 响应报文，使二者的始终维护错误的 ARP 表。

在 A 主机和 B 主机看来，彼此发送的数据包都是直接到达对方的，但在攻击者看来，其担当的就是“第三者”的角色。这种嗅探方法，也被称作“中间人”的方法。

➢ **ARP 泛洪攻击**

攻击者伪造大量不同 ARP 报文在同网段内进行广播，消耗网络带宽资源，造成网络速度急剧降低；同时，网关学习此类 ARP 报文，并更新 ARP 表，导致 ARP 表项被占满，无法学习合法用户的 ARP 表，导致合法用户无法访问外网。

在本交换机中，通过四元绑定功能在用户接入交换机时即对用户的四元信息进行绑定；而在 ARP 防护功能中则利用在交换机中绑定的四元信息对 ARP 报文进行检查，过滤非法 ARP 报文。通过上述两步可以很好的对局域网中 ARP 攻击进行防御。

本功能包括**防 ARP 欺骗**、**防 ARP 攻击**和**报文统计**三个功能配置页面。

11.2.1 防ARP欺骗

防 ARP 欺骗功能，通过四元绑定表对交换机收到的 ARP 报文进行检查，过滤非法的 ARP 报文，以此防御局域网中的 ARP 攻击。

进入页面的方法：**网络安全>>ARP 防护>>防 ARP 欺骗**

防ARP欺骗

防ARP欺骗： ○ 启用 ◉ 禁用

信任端口

☐ 1	☐ 2	☐ 3	☐ 4	☐ 5	☐ 6
☐ 7	☐ 8	☐ 9	☐ 10	☐ 11	☐ 12
☐ 13	☐ 14	☐ 15	☐ 16	☐ 17	☐ 18
☐ 19	☐ 20	☐ 21	☐ 22	☐ 23	☐ 24
☐ 25	☐ 26	☐ 27	☐ 28		

提交 全选 清空 帮助

注意：
信任端口为不进行防护的可信任端口，建议将上联端口和LAG端口设置为信任端口。

图11-13 防 ARP 欺骗

条目介绍：

➢ **防 ARP 欺骗**

防 ARP 欺骗： 选择启用并单击<提交>按键即可启用防 ARP 欺骗功能。

➢ 信任端口

信任端口： 勾选无须启用防 ARP 欺骗功能的信任端口。上联端口、路由端口以及 LAG 端口等特殊端口均应配置为信任端口。在启用防 ARP 欺骗功能之前，应先配置 ARP 信任端口，以免影响正常通信。

配置步骤：

步骤	操作	说明
1	绑定四元信息条目	必选操作。在**四元绑定**功能中将接入用户的四元信息进行绑定，手动绑定、扫描绑定和 DHCP 侦听方式均可进行绑定
2	对四元信息条目启用防护	必选操作。在**网络安全>>四元绑定>>绑定列表**页面中对相应的四元条目启用防护。
3	设置信任端口	必选操作。在**网络安全>>ARP 防护>>防 ARP 欺骗**页面中设置信任端口，上联端口、路由端口以及 LAG 端口等特殊端口均应配置为信任端口。
4	启用防 ARP 欺骗	必选操作。在**网络安全>>ARP 防护>>防 ARP 欺骗**页面中启用防 ARP 欺骗功能。

11.2.2 防ARP攻击

防 ARP 攻击功能对交换机的各端口处理的合法 ARP 数据包设定阀值，在单位时间内不可超过设定值。超过设定值时，交换机将停止处理 ARP 数据包 300 秒，能够有效的避免 ARP 泛洪攻击。

进入页面的方法：网络安全>>ARP 防护>>防 ARP 攻击



图11-14 防 ARP 攻击

条目介绍：

➢ **防 ARP 攻击配置**

端口选择：	点击<选择>按键，可根据所输端口号快速选择端口。
选择：	勾选端口配置端口防 ARP 攻击功能参数，可多选。
端口：	显示交换机的端口号。
防护功能：	选择是否启用防 ARP 攻击功能。
速率：	填写端口每秒允许接收的 ARP 数据包个数。
当前速率：	显示端口当前收到的 ARP 数据包速率。
状态：	显示端口当前防 ARP 攻击状态。
LAG：	显示端口当前所属的汇聚组。
操作：	点击<恢复>按键使端口恢复正常状态并重新启用防 ARP 攻击功能。

注意：

- 建议 LAG 端口不要开启防 ARP 攻击功能。

11.2.3 报文统计

通过报文统计功能，可以直观地查看各个端口收到的非法 ARP 数据包个数，并以此定位网络问题，并采取相应的防护措施。

进入页面的方法：网络安全>>ARP 防护>>报文统计



端口	信任端口	非法ARP报文	端口	信任端口	非法ARP报文
1	否	---	2	否	---
3	否	---	4	否	---
5	否	---	6	否	---
7	否	---	8	否	---
9	否	---	10	否	---
11	否	---	12	否	---
13	否	---	14	否	---
15	否	---	16	否	---
17	否	---	18	否	---
19	否	---	20	否	---
21	否	---	22	否	---
23	否	---	24	否	---

图11-15 报文统计

条目介绍：

➢ 自动刷新

自动刷新：	设置是否自动刷新端口统计情况。
刷新周期：	设置自动刷新周期。

➢ 非法 ARP 报文统计

端口：	显示交换机的端口号。
信任端口：	显示端口是否是 ARP 信任端口。
非法 ARP 报文：	显示端口收到的非法 ARP 数据包数量。

11.3 IP源防护

在本交换机中，通过四元绑定功能在用户接入交换机时即对用户的四元信息进行绑定；而在 IP 源防护功能中则利用在交换机中绑定的四元信息对 IP 包进行检查，过滤不符合四元绑定表的 IP 报文，只处理与四元绑定表吻合的数据包，提高交换机带宽资源的利用率。

进入页面的方法：网络安全>>IP 源防护>>报文统计



图11-16 IP 源防护

条目介绍：

➢ **IP 源防护配置**

端口选择：	点击<选择>按键，可根据所输端口号快速选择端口。
选择：	勾选端口配置端口的 IP 源防护功能，可多选。
端口：	显示交换机的端口号。
防护类型：	选择端口的防护类型。 ● 禁用：禁用端口的 IP 源防护功能。 ● SIP：只处理源 IP 地址和端口符合四元绑定信息的数据包。 ● SIP+MAC：只处理源 IP 地址、源 MAC 地址和端口均符合四元绑定信息的数据包。
LAG：	显示端口当前所属的汇聚组。

11.4 DoS防护

DoS（Denial of Service，拒绝服务）攻击是指攻击者利用网络协议实现的缺陷，耗尽被攻击对象的资源，使目标计算机或网络无法提供正常的服务或资源访问甚至崩溃。

DoS 攻击的具体的影响如下：

1) 耗尽服务器的资源，包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。使服务器疲于响应此类报文，导致网络瘫痪。

2) 由于交换机接收到此类报文需经过 CPU 处理，因此若请求报文数量过多，会导致交换机 CPU 利用率持续上升，无法正常工作。

本交换机通过解析IP数据包，分析数据包中的特定字段，并判断是否符合DoS攻击数据包的特征。对于非法的数据包，交换机将直接丢弃；而对于某些正常的数据包，由于流量过大可能导致受害主机瘫痪时，交换机可以对此类数据包进行限速。本交换机能够防护的DoS攻击种类如表11-1所示。

DoS 攻击类型	攻击特征
Land Attack	向目标主机发送一个特别伪造的 SYN 包，其 IP 源地址和目的地址都被设置为目标主机的 IP 地址，这种包可以造成被攻击主机因试图与自己建立连接而陷入死循环，从而很大程度上降低了系统性能。
Scan SYNFIN	TCP 标志位 SYN、FIN 位被置 1 的数据包。由于 SYN 标志用来初始化连接的，FIN 标志用来表示发端已完成发送任务请求关闭连接，所以 SYN/FIN 肯定是非法的数据包，本交换机能够识别此类攻击。
Xmascan	TCP 序号置为 0，FIN、URG、PSH 位置为 1 的数据包。
NULL Scan	TCP 序号置为 0，所有控制位置为 0 的数据包。在正常的 TCP 连接以及数据传输过程中，不会出现所有控制位置 0 的情况，此类数据包为非法的数据包。
SYN sPort less 1024	TCP SYN 标志位置 1，源端口小于 1024 的数据包。
Smurf Attack	通过冒充某主机向一个子网的广播地址发 ICMP 请求数据包，收到这一请求的主机都回应请求，向被攻击主机发包，使该主机受到攻击。
Blat Attack	数据包的 L4 源端口等于目的端口且 URG 置位。此攻击方式类似于 Land Attack，被攻击主机因尝试和自己建立连接使系统性能下降。
Ping Flooding	利用 Ping 广播风暴，淹没整个目标系统，以至于该系统不能响应合法的通信。
SYN/SYN-ACK Flooding	每当我们进行一次标准的 TCP 连接，都会有一个三次握手的过程，而 TCP-SYN Flood 只进行前两个步骤，服务方在一定时间内等待请求方 ASK 消息。由于一台服务器可用的 TCP 连接是有限的，如果攻击方发送大量此类连接请求，则服务方 TCP 连接队列将会很快阻塞，系统资源和可用带宽急剧下降，无法提供正常的网络服务，从而造成拒绝服务。
winNuke Attack	利用操作系统漏洞，向目标主机的 TCP 139 端口（NetBIOS）发送数据，可导致机器蓝屏。主要利用的是 TCP 包中的 URG(Urgent Pointer，紧急指针)，有漏洞的操作系统不能正确处理这一标志。

表11-1 本交换机支持的 DoS 防护种类

11.4.1 DoS防护

在此页面中可以根据实际需要启用合适的 DoS 防护策略。

进入页面的方法：网络安全**>>DoS 防护>> DoS 防护**



图11-17 DoS 防护

条目介绍：

➤ 全局配置

DoS 攻击防护： 选择是否启用交换机的 DoS 防护功能。

Ping 限速： 启用了 Ping Flooding 攻击防护后，可在此设置局域网中 ping 数据包的转发速度。

SYN 限速： 启用了 SYN/SYN-ACK Flooding 攻击防护后，可在此设置局域网中 SYN/SYN-ACK 数据包的转发速度。

➤ 攻击防护列表

选择： 勾选启用相应 DoS 防护。

防护类型： 显示防护类型。

攻击次数统计： 显示交换机受到的相应攻击类型的攻击总次数。

11.4.2 攻击检测

在此页面中可以检测交换机受到 DoS 攻击的实时信息。

进入页面的方法：网络安全>>**DoS** 防护>>**DoS** 防护



图11-18 攻击检测

条目介绍：

➢ 检测时间

检测时间：	配置检测攻击时的检测时间长度，检测类型不包括泛洪攻击。
检测：	点击<检测>按键开始检测，交换机采用轮询方式检测受到的各种DoS 攻击实时情况。

➢ 检测结果

端口：	显示交换机端口号。
攻击类型：	显示攻击类型名称。
已检测攻击次数：	显示在上一检测时间内受到的实时攻击次数。



说明：

- 还可以从以下三方面对 DoS 攻击进行防护，以进一步保证网络安全。

1) 检查并修补系统漏洞，及时安装系统补丁程序，对于重要信息要建立和完善备份机制。
2) 作为网络管理员，可检查系统的物理环境，禁止一些不必要的网络服务。
3) 利用硬件防火墙等网络安全设备提高网络的安全性。

11.5 802.1X认证

802.1X 协议是 IEEE802 LAN/WAN 委员会为了解决无线局域网网络安全问题提出的。后来该协议作为局域网端口的一个普通接入控制机制应用于以太网中，主要用于解决以太网内认证和安全方面的问题，在局域网接入设备的端口这一级对所接入的设备进行认证和控制。

本交换机可以作为一个认证系统来对网络中的计算机进行认证。连接在端口上的用户设备如果能通过交换机认证，就可以访问局域网中的资源；如果不能通过交换机认证，则无法访问局域网中的资源。

➢ **802.1X 体系结构**

802.1X的系统是采用典型的Client/Server体系结构，包括三个实体，如图11-19所示。

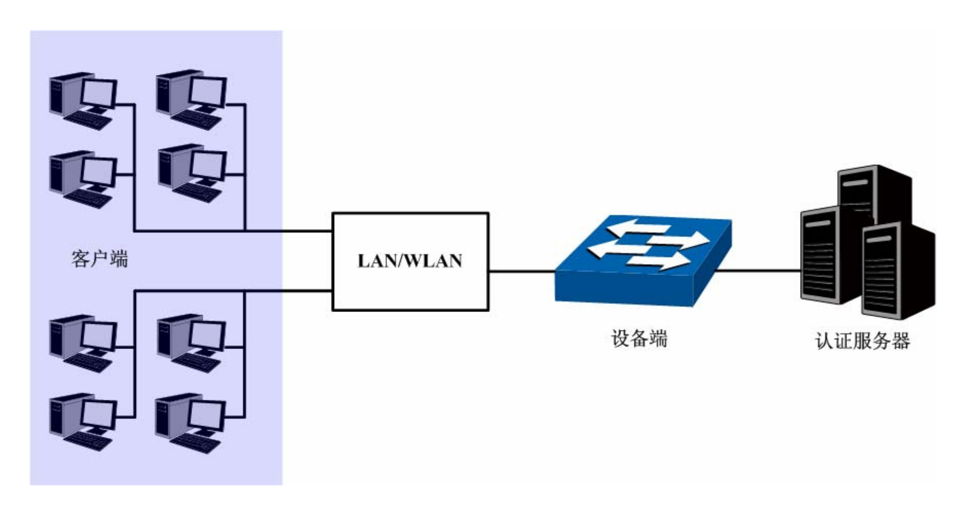


图11-19 802.1X 认证的体系结构

1) 客户端：局域网中的一个实体，多为普通计算机，用户通过客户端软件发起 802.1X 认证，并由设备端对其进行认证。客户端软件必须为支持 802.1X 认证的用户终端设备。

2) 设备端：通常为支持 802.1X 协议的网络设备，如本交换机，为客户端提供接入局域网的物理/逻辑端口，并对客户端进行认证。

3) 认证服务器：为设备端提供认证服务的实体，例如可以使用 RADIUS 服务器来实现认证服务器的认证和授权功能。该服务器可以存储客户端的相关信息，并实现对客户端的认证和授权。为了保证认证系统的稳定，可以为网络设置一个备份认证服务器。当主认证服务器出现故障时，备份认证服务器可以接替认证服务器的工作，保证认证系统的稳定。

➢ **802.1X 认证工作机制**

IEEE 802.1X 认证系统使用 EAP（Extensible Authentication Protocol，可扩展认证协议）来实现客户端、设备端和认证服务器之间认证信息的交换。

1) 在客户端与设备端之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。

2) 在设备端与 RADIUS 服务器之间，可以使用两种方式来交换信息。一种是 EAP 协议报文使用 EAPOR（EAP over RADIUS）封装格式承载于 RADIUS 协议中；另一种是设备端终结 EAP 协议报文，采用包含 PAP（Password Authentication Protocol，密码验证协议）或 CHAP（Challenge Handshake Authentication Protocol，质询握手验证协议）属性的报文与 RADIUS 服务器进行认证。

3) 当用户通过认证后，认证服务器会把用户的相关信息传递给设备端，设备端根据 RADIUS 服务器的指示（Accept 或 Reject）决定受控端口的授权/非授权状态。

➢ **802.1X 认证过程**

认证过程可以由客户端主动发起，也可以由设备端发起。一方面当设备端探测到有未经过认证的用户使用网络时，就会主动向客户端发送 EAP-Request/Identity 报文，发起认证；另一方面客户端可以通过客户端软件向设备端发送 EAPOL-Start 报文，发起认证。

802.1X 系统支持 EAP 中继方式和 EAP 终结方式与远端 RADIUS 服务器交互完成认证。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

1. EAP 中继方式

EAP中继方式是IEEE 802.1X标准规定的，将EAP（扩展认证协议）承载在其它高层协议中，如EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP中继方式需要RADIUS服务器支持EAP属性：EAP-Message和Message-Authenticator。本交换机支持的EAP中继方式是EAP-MD5，EAP-MD5 认证过程如图11-20所示。

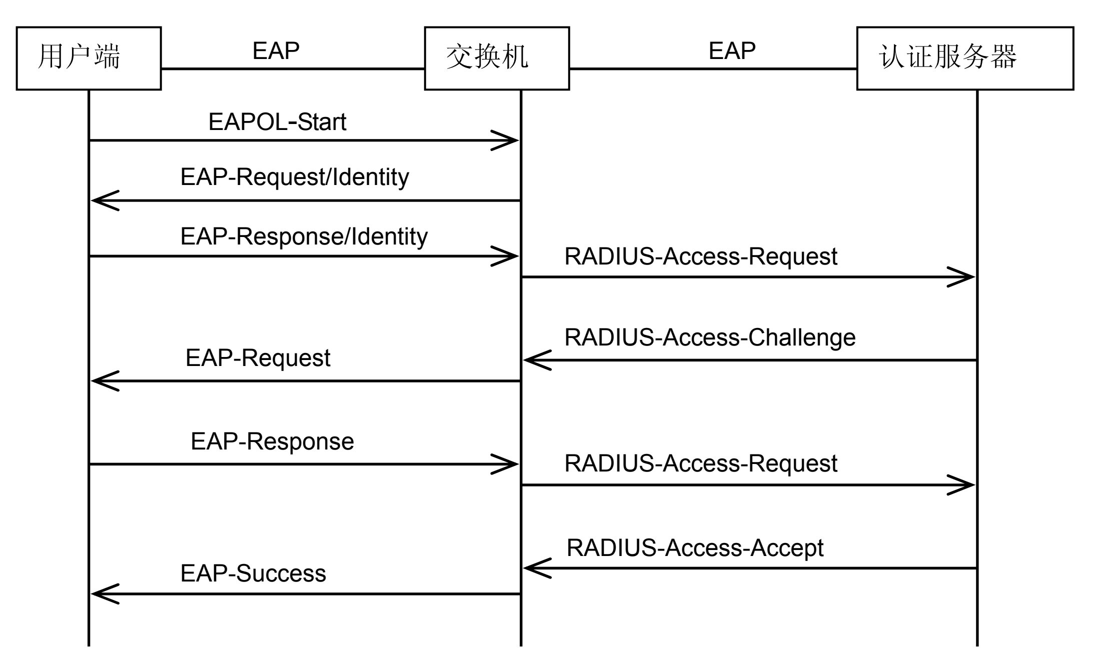


图11-20 EAP-MD5 认证过程

1) 当用户有访问网络需求时打开 802.1X 客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求（EAPOL-Start 报文）。此时，客户端程序将发出请求认证的报文给设备端，开始启动一次认证过程。

2) 设备端收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）要求用户的客户端程序发送输入的用户名。

3) 客户端程序响应设备端发出的请求， 将用户名信息通过数据帧（EAP-Response/Identity 报文）发送给设备端。设备端将客户端发送的数据帧经过封包处理后（RADIUS Access-Request 报文）送给认证服务器进行处理。

4) RADIUS 服务器收到设备端转发的用户名信息后，将该信息与数据库中的用户名表对比，找到该用户名对应的密码信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过 RADIUS Access-Challenge 报文发送给设备端，由设备端转发给客户端程序。

5) 客户端程序收到由设备端传来的加密字（EAP-Request/MD5 Challenge 报文）后，用该加密字对密码部分进行加密处理（此种加密算法通常是不可逆的，生成 EAP-Response/MD5 Challenge 报文），并通过设备端传给认证服务器。

6) RADIUS 服务器将收到的已加密的密码信息（RADIUS Access-Request 报文）和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文）。

7) 设备收到认证通过消息后将端口改为授权状态，允许用户通过端口访问网络。在此期间，设备端会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。缺省情况下，两次握手请求报文都得不到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。

8) 客户端也可以发送 EAPOL-Logoff 报文给设备端，主动要求下线，设备端把端口状态从授权状态改变成未授权状态。

2. EAP 终结方式

EAP终结方式将EAP报文在设备端终结并映射到RADIUS报文中，利用标准RADIUS协议完成认证、授权和计费。设备端与RADIUS服务器之间可以采用PAP或者CHAP认证方法。本交换机支持的EAP终结方式是PAP，PAP认证过程如图11-21所示。

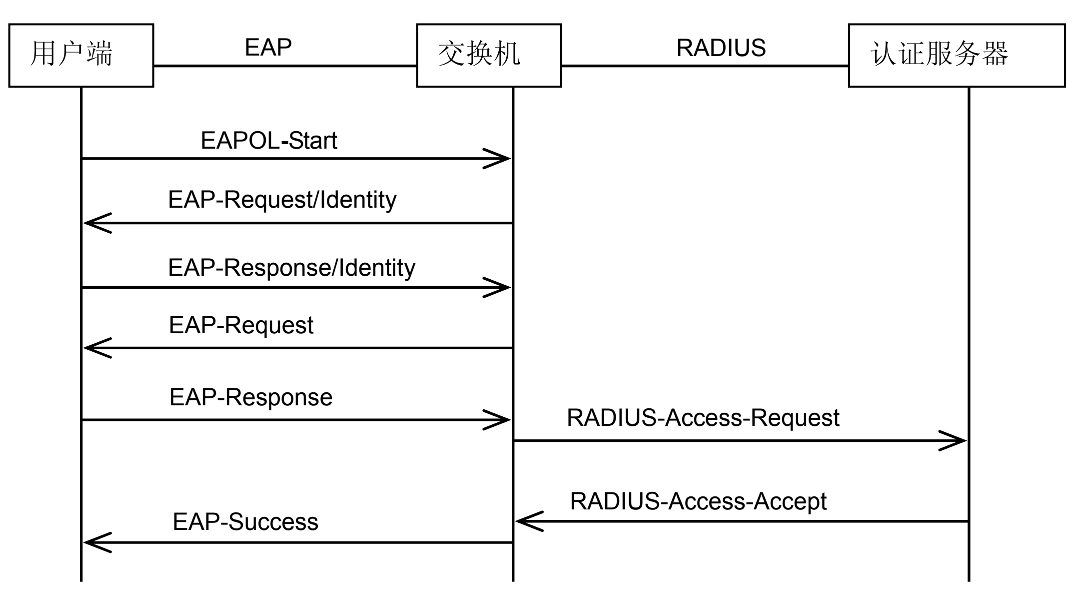


图11-21 PAP 认证过程

在 PAP 模式中，交换机对用户口令信息进行加密，然后把用户名、随机加密字和客户端加密后的口令信息一起转发给认证服务器进行相关的认证处理；而在 EAP-MD5 模式中，随机加密字由认证服务器产生，交换机只负责把认证信息报文封装后转发。

➢ **802.1X 定时器**

802.1X 认证过程中会启动多个定时器以控制接入用户、设备以及 RADIUS 服务器之间进行合理、有序的交互。本交换机中的 802.1X 定时器主要有以下三种：

1) **客户端认证超时定时器：**当交换机向客户端发送报文后，交换机启动此定时器，若在该定时器设置的时长内，交换机没有收到客户端的响应，交换机将重发该报文。

2) **认证服务器超时定时器：**当交换机向认证服务器发送报文后，交换机启动此定时器，若在该定时器设置的时长内，交换机没有收到认证服务器的响应，交换机将重发认证请求报文。

3) **静默定时器：**对用户认证失败以后，交换机需要静默一段时间（该时间由静默定时器设置），在静默期间，交换机不再处理该用户的认证请求。

➢ **Guest VLAN**

Guest VLAN 功能用来允许未通过认证的用户访问某些特定资源。用户认证端口在通过 802.1X 认证之前属于一个缺省 VLAN（即 Guest VLAN），用户访问该 VLAN 内的资源不需要认证，但此时不能够访问其它网络资源；认证成功后，端口离开 Guest VLAN，用户可以访问其它的网络资源。

用户可以在 Guest VLAN 中获取 802.1X 客户端软件、升级客户端或执行其它一些用户升级程序。如果因为没有专用的认证客户端或者客户端版本过低等原因，导致一定的时间内端口上无客户端认证成功，本交换机会把该端口加入到 Guest VLAN。

开启 802.1X 特性并正确配置 Guest VLAN 后，当交换机向客户端发送 EAP-Request/Identity 报文而没有收到客户端的回应时，该端口将按照各自的链路类型被加入到 Guest VLAN 内。此时如果 Guest VLAN 中有用户发起认证且认证失败，相应连接端口仍会留在 Guest VLAN 内；如果认证成功，端口离开 Guest VLAN，加入配置的 VLAN 中。用户下线后，端口将返回 Guest VLAN 中。

本交换机 802.1X 认证功能包括**全局配置**、**端口配置**和 **RADIUS 配置**三个配置页面。

11.5.1 全局配置

在全局配置功能页面，可以开启全局 802.1X 认证功能，选择本交换机提供的认证方法，并设置 Guest VLAN 以及各种定时器来协调整个系统的 802.1X 认证过程。

进入页面的方法：网络安全>>802.1X 认证>>全局配置

全局配置

802.1X功能： ○ 启用 ⦿ 禁用
认证方法： EAP-MD5
Guest VLAN： ○ 启用 ⦿ 禁用
Guest VLAN ID： 0 （2-4094）
提交

认证参数配置

静默： ○ 启用 ⦿ 禁用
静默时长： 10 秒（1-999）
重复发送次数： 3 次（1-9）
客户端响应超时： 3 秒（1-9）
服务器响应超时： 3 秒（1-9）
提交
帮助

图11-22 全局配置

条目介绍：

➢ 全局配置

802.1X 功能： 选择是否启用 802.1X 认证功能。

认证方法： 选择 802.1X 认证方法。

- EAP-MD5：交换机与认证服务器之间运行 EAP 协议，EAP 帧中封装认证数据，将该协议承载在其它高层次协议中(如 RADIUS)，以便穿越复杂的网络到达认证服务器。
- PAP：用户端与交换机之间运行 EAP 协议，交换机将 EAP 消息转换为其它认证协议(如 RADIUS)，传递用户认证信息给认证服务器系统。

Guest VLAN： 选择是否启用 Guest VLAN 功能。

Guest VLAN ID： 填写启用 Guest VLAN 的 VLAN ID。Guest VLAN 中的用户可以访问指定的网络资源。

➢ 认证参数配置

静默： 选择是否启用静默计时器。

静默时长： 填写静默时长。用户认证失败后，在静默时间内不再处理同一用户的 802.1X 认证请求。

重复发送次数： 填写认证报文的最大重传次数。

客户端响应超时： 填写交换机等待客户端响应的最大等待时间。若交换机在设定时间内没有收到客户端的回复，则重发报文。

服务器响应超时： 填写交换机等待服务器响应的最大等待时间。若交换机在设定时间内没有收到服务器的回复，则重发报文。

11.5.2 端口配置

在端口配置功能页面，可以根据实际的网络情况设置端口的 802.1X 功能特性。

进入页面的方法：网络安全**>>802.1X** 认证**>>**端口配置

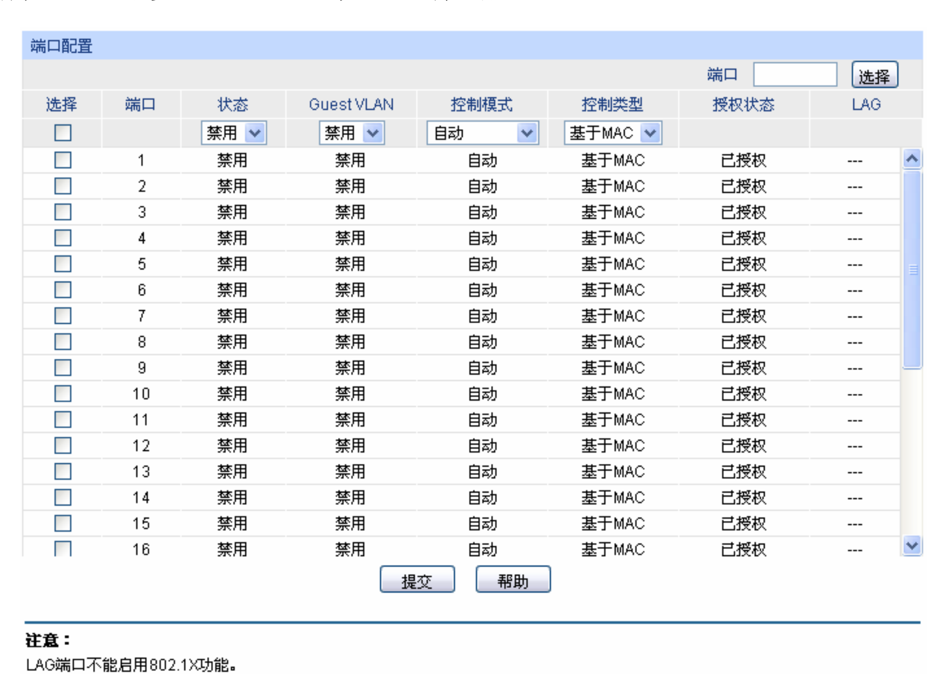


图11-23 端口配置

条目介绍：

➢ 端口配置

端口选择： 点击<选择>按键，可根据所输端口号快速查找相应条目。

选择： 勾选端口，配置端口的 802.1X 认证状态，可多选。

端口： 显示交换机端口号。

状态： 选择该端口是否启用 802.1X 认证。

Guest VLAN： 选择该端口是否启用 Guest VLAN。

控制模式： 选择该端口的控制模式。

- 自动：端口需要进行认证。
- 强制已认证：端口不需要认证即可访问网络。
- 强制不认证：端口永远无法通过认证。

控制类型： 选择该端口的控制类型。

- 基于 MAC：该端口连接的所有计算机都需要认证。
- 基于 Port：该端口连接的某个用户通过认证后，其它用户均无须认证即可访问网络。

授权状态： 显示此端口的授权状态。

LAG： 显示端口当前所属的汇聚组。

11.5.3 RADIUS配置

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）认证服务器为交换机提供认证服务，其存储有关用户的信息，包括用户名、密码以及其它参数，用于实现对用户进行认证、授权和计费。RADIUS 配置功能页面用来设置网络中认证服务器的参数，保证认证过程通畅有序的进行。

进入页面的方法：网络安全>>**802.1X** 认证>>**RADIUS** 配置

认证服务器配置
服务器IP： 0.0.0.0 （格式为192.168.0.1）
备份服务器IP： 0.0.0.0 （格式为192.168.0.1）
认证端口： 1812 （1-65535）
授权共享密钥：
提交

计费服务器配置
计费功能： 启用 禁用
服务器IP： 0.0.0.0 （格式为192.168.0.1）
备份服务器IP： 0.0.0.0 （格式为192.168.0.1）
计费端口： 1813 （1-65535）
授权共享密钥：
提交
帮助

图11-24 RADIUS 配置

条目介绍：

➢ 认证服务器配置

服务器 IP： 填写认证服务器的 IP 地址。

备份服务器 IP： 填写备份认证服务器的 IP 地址。

认证端口： 填写认证服务器提供认证服务的协议端口。

授权共享密钥： 填写交换机与服务器共享的密钥。

➢ 计费服务器配置

计费功能： 选择是否启用计费功能。

服务器 IP： 填写计费服务器的 IP 地址。

备份服务器 IP： 填写备份计费服务器的 IP 地址。

计费端口： 填写计费服务器提供计费服务的协议端口。

授权共享密钥： 填写交换机与服务器共享的密钥。

注意：

- 只有同时开启全局和端口的 802.1X 特性后，才能使 802.1X 认证功能生效。
- LAG 端口不能启用 802.1X 功能。如果端口启动了 802.1X，则不能配置该端口加入聚合组。
- 认证服务器连接的端口请勿开启 802.1X 特性，且服务器配置参数必须与认证服务器软件的参数一致。

配置步骤：

步骤	操作	说明
1	搭建认证服务器	必选操作。搭建完成后，请在服务器中记录局域网接入用户的信息并设置相应的用户名和密码以备认证。
2	安装客户端软件	必选操作。请在接入计算机中安装光盘中的 802.1X客户端软件，安装过程见附录A 802.1X客户端软件使用说明。
3	设置 802.1X 全局参数	必选操作。默认情况下，交换机 802.1X 全局功能未开启，请在**网络安全>>802.1X 认证>>全局配置**页面中设置全局参数。
4	设置认证服务器参数	必选操作。请自行搭建认证服务器，并在**网络安全>>802.1X 认证>>RADIUS 配置**页面中设置服务器参数。
5	设置各端口 802.1X 功能参数	必选操作。请在**网络安全>>802.1X 认证>>端口配置**页面中根据实际网络情况设置交换机各端口的 802.1X 功能参数。

回目录

第12章 SNMP

➢ **SNMP 概述**

SNMP（Simple Network Management Protocol，简单网络管理协议）是目前 UDP/IP 网络中应用最为广泛的网络管理协议，它提供了一个管理框架来监控和维护互联网设备。SNMP 结构简单，使用方便，并且能够屏蔽不同设备的物理差异，实现对不同设备的自动化管理，所以得到了广泛的支持和应用，目前大多数网络管理系统和平台都是基于 SNMP 的。

SNMP 的最大优势就是设计简单，他既不需要复杂的实现过程，也不会占用太多的网络资源，便于使用。SNMP 的基本功能包括监视网络性能、检测分析网络差错和配置网络设备等。在网络正常工作时，SNMP 可实现统计、配置和测试等功能；当网络出故障时，可实现各种错误检测和恢复功能。

➢ **SNMP 的管理框架**

SNMP 包括三个网络元素：SNMP 管理者(SNMP Manager)，SNMP 代理(SNMP Agent)，MIB 库（Management Information Base，管理信息库）。

SNMP 管理者：运行在 SNMP 客户端程序的工作站，提供了非常友好的人机交互页面，方便网络管理员完成绝大多数的网络设备管理工作。

SNMP 代理：驻留在被管理设备上的一个进程，负责接受、处理来自 SNMP 管理者的请求报文。在一些紧急情况下，SNMP 代理也会通知 SNMP 管理者事件的变化。

MIB 库：被管理对象的集合。它定义了被管理对象的一系列的属性：对象的名字、对象的访问权限和对象的数据类型等。每个 SNMP 代理都有自己的 MIB。SNMP 管理者根据权限可以对 MIB 中的对象进行读/写操作。

SNMP管理者是SNMP网络的管理者，SNMP代理是SNMP网络的被管理者，他们之间通过SNMP协议来交互管理信息。SNMP管理者、SNMP代理、MIB库三者的关系如图 12-1所示。

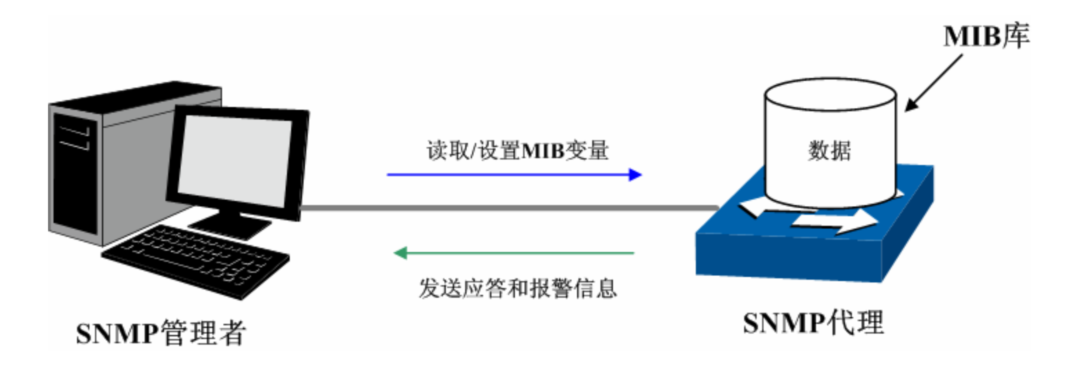


图 12-1 SNMP 网元关系图

➢ **SNMP 的协议版本**

本交换机提供了 SNMPv3 的管理功能，同时兼容 SNMPv1 和 SNMPv2c，SNMP 管理者和 SNMP 代理的 SNMP 版本需要一致，它们之间才能相互通信，可以根据自己的应用需求，选择不同安全级别的管理模式。

SNMPv1：采用团体名（Community Name）认证。团体名用来定义 SNMP 管理者和 SNMP 代理的关系。如果 SNMP 报文携带的团体名没有得到设备的认可，该报文将被丢弃。团体名起到了类似于密码的作用，用来限制 SNMP 管理者对 SNMP 代理的访问。

SNMPv2c：也采用团体名认证。它在兼容 SNMPv1 的同时又扩充了 SNMPv1 的功能。

SNMPv3：SNMPv3 在前两个版本 v1、v2c 的基础上大大加强了安全性和用户可控制性，他采用了 VACM（View-based Access Control Model，基于视图的访问控制模型）及 USM（User-Based Security Model，基于用户的安全模型）的认证机制。用户可以设置认证和加密功能，认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 SNMP 管理者和 SNMP 代理之间的传输报文进行加密，以免被窃听。通过有无认证和有无加密等功能组合，可以为 SNMP 管理者和 SNMP 代理之间的通信提供更高的安全性。

➢ **MIB 库简介**

MIB是以树状结构进行存储的。树的节点表示被管理对象，它可以用从根开始的一条路径唯一地识别，被管理对象可以用一串数字唯一确定，这串数字是被管理对象的OID（Object Identifier，对象标识符）。MIB的结构如图 12-2所示。图中，B的OID为{1.2.1.1}，A的OID为{1.2.1.1.5}。

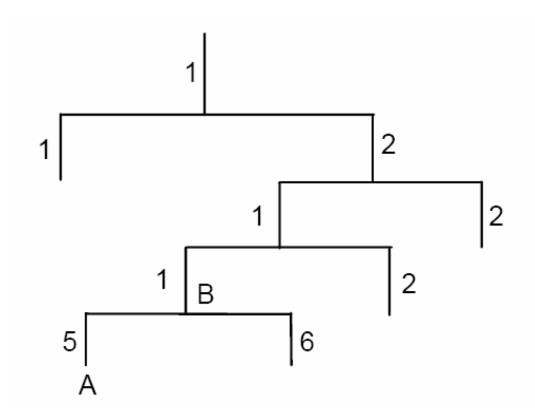


图 12-2 MIB 树结构

➢ **SNMP 配置概要**

● 创建视图

MIB 视图是全部 MIB 管理对象的一个子集。管理对象以 OID（Object Identifier，对象标识符）来表示，通过配置管理对象的视图类型（包括/排除），来达到控制该管理对象能否被管理的目的。各管理对象的 OID 可以在 SNMP 管理软件上找到。

● 创建 SNMP 组

创建完视图之后，需要创建 SNMP 组，只有“组名”、“安全模式”、“安全级别”三项均相同的组，才被认为是同一个组。同时可以为各个 SNMP 组添加只读/只写/通知视图，从而满足了处于不同组内的用户对交换机功能的访问权限不同的需求。

● 创建用户

用户创建于 SNMP 组中，SNMP 管理端使用此处创建的用户及其认证/加密密码来登录 SNMP 代理端。

SNMP 模块主要用于配置交换机的 SNMP 功能，包括 **SNMP 配置**和**通知管理**两个部分。

12.1 SNMP配置

在本功能处可以配置 SNMP 的各项基本功能，包括**全局配置**、**视图管理**、**组管理**、**用户管理**和**团体管理**五个配置页面。

12.1.1 全局配置

配置交换机的 SNMP 功能，首先需要在本页配置交换机 SNMP 的全局功能。

进入页面的方法：**SNMP>>SNMP 配置>>全局配置**

全局配置

SNMP功能： ○ 启用 ◉ 禁用 提交

本地引擎配置

本地引擎ID： 80002e57030077c66e2d8f （10-64个十六进制字符） 默认ID 提交

远程引擎配置

远程引擎ID： （0或10-64个十六进制字符） 提交 帮助

注意：
引擎ID的字符个数必须为偶数。

图 12-3 全局配置

条目介绍：

➢ 全局配置

SNMP 功能： 选择是否启用交换机的 SNMP 功能。

➢ 本地引擎配置

本地引擎 ID： 填写本地 SNMP 实体的引擎 ID。本地用户建立在本地引擎之下。

➢ 远程引擎配置

远程引擎 ID： 填写 SNMP 管理端的引擎 ID。远程用户建立在远程引擎之下。

注意：

- 引擎 ID 的字符个数必须为偶数。

12.1.2 视图管理

在 SNMP 报文中使用管理变量(OID)来描述交换机中的管理对象，MIB（Management Information Base，管理信息库）是所监控网络设备的管理变量的集合。视图用来控制管理变量是如何被管理的。本页用来配置 SNMP 的视图。

进入页面的方法：**SNMP>>SNMP 配置>>视图管理**



图 12-4 视图管理

条目介绍：

➢ 新建视图

视图名称： 填写视图条目的名称。一个视图可以有多个同名的视图条目。

MIB 子树 OID： 填写该视图条目的管理变量（OID）。

视图类型： 选择 OID 的类型。

- 包括：该 OID 可以被管理软件管理。
- 排除：该 OID 不能被管理软件管理。

➢ 视图列表

选择： 勾选条目进行删除。同一视图下的所有视图条目会被同时选择。

视图名称： 显示视图名称。

类型： 显示对应 OID 的类型。

MIB 子树 OID： 显示对应视图下的管理变量（OID）。

12.1.3 组管理

本页用来配置 SNMP 的组，组内的用户通过只读、只写、通知视图来达到访问控制的目的。

进入页面的方法：**SNMP>>SNMP 配置>>组管理**

组配置

组名： （1-16个字符）

安全模式： v1

安全级别： noAuthNoPriv

只读视图： viewDefault

只写视图： None

通知视图： None

添加 清空

组列表

选择	组名	安全模式	安全级别	只读视图	只写视图	通知视图	操作

全选 删除 帮助

注意：

一个组必须具备一个只读视图，默认只读视图为viewDefault。

图 12-5 组管理

条目介绍：

➢ 组配置

组名： 填写组名。与“安全模式”和“安全级别”三项共同组成该组的标识，三项均相同才被认为是同一组。

安全模式： 选择组的安全模式。

- v1：SNMP v1，采用团体名（Community Name）认证，也可以在**团体管理**页面直接进行配置。
- v2C：SNMP v2C，采用团体名（Community Name）认证，也可以在**团体管理**页面直接进行配置。
- v3：SNMP v3，采用 USM 认证。

安全级别： 选择 SNMP v3 的组的安全级别。

- noAuthNoPriv：不认证不加密。
- authNoPriv：认证不加密。
- authPriv：认证加密。

只读视图： 选择只读视图，对所选的视图只能被查看不能被编辑。

只写视图： 选择只写视图，对所选的视图只能被编辑不能被查看。若您想要进行读写操作，则需要同时在“只读视图”中添加。

通知视图： 选择通知视图，管理软件可以接收到所选视图发送的异常警报信息。

➢ 组列表

选择： 勾选条目进行删除，可多选。

组名： 显示 SNMP 组的组名。

安全模式： 显示组的安全模式。

安全级别： 显示组的安全级别。

只读视图： 显示组中具有只读权限的视图名称。

只写视图： 显示组中具有只写权限的视图名称。

通知视图： 显示组中具有通知权限的视图名称。

操作： 点击对应条目的<编辑>按键，可以修改该条目的视图。修改完毕后点击<修改>按键，修改内容生效。

注意：

- 一个组必须具备一个只读视图，默认只读视图为 viewDefault。

12.1.4 用户管理

SNMP 管理软件可以通过用户的方式对交换机进行管理。用户建立在组之下，与其所属的组具有相同的安全级别和访问控制权限。本页用来配置 SNMP 的用户。

进入页面的方法：**SNMP>>SNMP 配置>>用户管理**

用户配置

用户名：	admin （1-16个字符）		
用户类型：	本地用户	组名：	
安全模式：	v1	安全级别：	noAuthNoPriv
认证模式：	None	认证密码：	●●●●● （1-16个字符）
加密模式：	None	加密密码：	（1-16个字符）

添加 清空

用户列表

选择	用户名	用户类型	组名	安全模式	安全级别	认证模式	加密模式	操作

全选 删除 帮助

注意：
用户的安全模式、安全级别必须和其所属组的安全模式、安全级别相同。

图 12-6 用户管理

条目介绍：

➢ 用户配置

用户名： 填写用户名。

用户类型： 选择用户类型。

- 本地用户：建立在本地引擎下的用户。
- 远程用户：建立在远程引擎下的用户。

组名： 选择组名。通过“组名”、“安全模式”、“安全级别”来确定用户所属的组。

安全模式： 选择安全模式。

安全级别： 选择安全级别。

认证模式： 选择 SNMP v3 用户的认证模式。

- None：不认证。
- MD5：信息摘要算法。
- SHA：安全散列算法，比 MD5 的安全性更高。

认证密码： 输入认证密码。

加密模式： 选择 SNMP v3 用户的加密模式。

- None：不加密。
- DES：数据加密标准。

加密密码： 输入加密密码。

➢ 用户列表

选择： 勾选条目进行删除，可多选。

用户名： 显示用户名。

用户类型： 显示用户类型。

组名： 显示组名。

安全模式： 显示安全模式。

安全级别： 显示安全级别。

认证模式： 显示认证模式。

加密模式： 显示加密模式。

操作： 点击对应条目的<编辑>按键，可以修改该用户所属的组。修改完毕后点击<修改>按键，修改内容生效。

注意：

- 用户的安全模式、安全级别必须和其所属组的安全模式、安全级别相同。

12.1.5 团体管理

SNMP v1 和 SNMP v2C 采用团体名（Community Name）认证，团体名起到了类似于密码的作用。若您使用的是 SNMP v1 和 SNMP v2C，配置完视图之后，可以直接在本页配置 SNMP 的团体。

进入页面的方法：**SNMP>>SNMP 配置>>团体管理**

团体配置

团体名： （1-16个字符） 添加

权限： read-only 清空

MIB视图： viewDefault

团体列表

选择	团体名	权限	MIB视图	操作

全选 删除 帮助

注意：
团体的默认MIB视图为viewDefault。

图 12-7 团体管理

条目介绍：

➢ 团体配置

团体名：	填写团体名。
权限：	选择该团体对视图的访问权限。 ● read-only：团体对相应视图具有只读权限。 ● read-write：团体对相应视图具有读写权限。
MIB 视图：	选择团体可访问的视图。

➢ 团体列表

选择：	勾选条目进行删除，可多选。
团体名：	显示团体名。
权限：	显示团体对视图的访问权限。
MIB 视图：	显示团体可访问的视图。
操作：	点击对应条目的<编辑>按键，可以修改该团体的访问视图及访问权限。修改完毕后点击<修改>按键，修改内容生效。

注意：

● 团体的默认 MIB 视图为 viewDefault。

SNMP 功能配置步骤：

● 若您使用 SNMPv3 版本

步骤	操作	说明
1	启用 SNMP 全局功能	必选操作。在 **SNMP>>SNMP 配置>>全局配置**页面，启用交换机的 SNMP 功能。

<table>
<tr><td>2</td><td>创建视图</td><td>可选操作。在 SNMP>>SNMP 配置>>视图管理页面，创建管理对象的视图。默认视图名为 viewDefault，OID 为 1。</td></tr>
<tr><td>3</td><td>创建 SNMP 组</td><td>必选操作。在 SNMP>>SNMP 配置>>组管理页面，创建 SNMPv3 类型的组，并为组添加不同访问权限的视图。</td></tr>
<tr><td>4</td><td>创建 SNMP 组内的用户</td><td>必选操作。在 SNMP>>SNMP 配置>>用户管理页面，创建 SNMPv3 组内的用户，并配置用户的认证/加密模式及密码。</td></tr>
</table>

- 若您使用 SNMPv1 版本或 SNMPv2c 版本

<table>
<tr><th>步骤</th><th colspan="3">操作</th><th>说明</th></tr>
<tr><td>1</td><td colspan="3">启用 SNMP 全局功能。</td><td>必选操作。在 SNMP>>SNMP 配置>>全局配置页面，启用交换机的 SNMP 功能。</td></tr>
<tr><td>2</td><td colspan="3">创建视图</td><td>可选操作。在 SNMP>>SNMP 配置>>视图管理页面，创建管理对象的视图。默认视图名为 viewDefault，OID 为 1。</td></tr>
<tr><td rowspan="3">3</td><td rowspan="3">配置访问权限</td><td>直接设置</td><td>创建团体</td><td rowspan="3">二者必选其一。
• 直接设置是在 SNMP>>SNMP 配置>>团体管理页面，以 SNMPv1 和 v2c 版本的团体名进行设置。
• 间接设置采用与 SNMPv3 版本一致的命令形式，添加用户到 v1/v2c 类型的组，即相当于 SNMPv1 和 SNMPv2c 版本的团体名。在 SNMP 管理软件上用来登录交换机的团体名需要跟这里配置的用户名一致，该组下创建的 v1/v2c 用户（团体）的读、写视图与该组的读写视图对应。</td></tr>
<tr><td rowspan="2">间接设置</td><td>创建 SNMP 组</td></tr>
<tr><td>创建 SNMP 组内的用户</td></tr>
</table>

12.2 通知管理

通知管理功能是交换机主动向管理软件报告某些视图的重要事件（如设备重启等），便于管理员通过管理软件对交换机一些特定事件进行及时监控和处理。

通知报文分为以下两种：

Trap：发送 Trap 报文通知 SNMP 管理者。

Inform：发送 Inform 报文通知 SNMP 管理者，并且要求 SNMP 管理者返回信息。交换机发送 Inform 报文后，若经过超时时间仍没有收到 Inform 回应报文，则会重发 Inform 报文。超过重传次数后，将不再重复发送该 Inform 报文。Inform 具有更高的可靠性，在 SNMP v2c 和 SNMP v3 中均可以使用。

本页用来配置 SNMP 的通知管理功能。

进入页面的方法：**SNMP>>通知管理>>通知管理**

新建条目
目的IP地址： UDP端口： 162
团体名/用户名：
安全模式： v1 安全级别： noAuthNoPriv 添加
通知类型： Trap 清空
重传： （1-255）
超时： 秒（1-3600）

目的主机列表

选择	目的IP地址	UDP端口	团体名/用户名	安全模型	安全级别	通知类型	超时	重传	操作

全选 删除 帮助

图 12-8 通知管理

条目介绍：

➢ 新建条目

目的 IP 地址： 填写管理主机的 IP 地址。

UDP 端口： 填写管理主机上启用供通知过程使用的 UDP 端口，与 IP 地址共同作用。默认为 162。

团体名/用户名： 配置管理软件的团体名/用户名。

安全模式： 选择用户的安全模式。

安全级别： 配置 SNMP v3 的用户的安全级别。

- noAuthNoPriv：不认证不加密。
- authNoPriv：认证不加密。
- authPriv：认证加密。

通知类型： 选择使用的通知报文的类型。

- Trap：以 Trap 方式发送通知。
- Inform：以 Inform 方式发送通知，Inform 具有更高的可靠性。

重传： 填写 Inform 报文的重传次数。交换机发送 Inform 报文后，若经过超时时间仍没有收到 Inform 回应报文，则会重发 Inform 报文。超过重传次数后，将不再重复发送 Inform 报文。默认为 3。

超时： 填写交换机等待 Inform 回应报文的时间。超过该时间后，将重新发送 Inform 报文。默认为 100 秒。

➢ 目的主机列表

选择： 勾选条目进行删除，可多选。

目的 IP 地址： 显示管理主机的 IP 地址。

UDP 端口： 显示管理主机上启用供通知过程使用的 UDP 端口。

团体名/用户名： 显示管理软件的团体名/用户名。

安全模型： 显示用户的安全模式。

安全级别： 显示 SNMP v3 的用户的安全级别。

通知类型： 显示使用的通知报文的类型。

超时： 显示 Inform 报文的重传次数。

重传： 显示收到 Inform 报文回应报文的超时时间。

操作： 点击对应条目的<编辑>按键，可以修改该通知条目的参数。修改完毕后点击<修改>按键，修改内容生效。

12.3 RMON

RMON（Remote Monitoring，远程网络监视）完全基于SNMP 体系结构，是IETF（Internet Engineering Task Force，因特网工程任务组 ）提出的标准监控规范，他使SNMP更为有效、更为积极主动地监控远程设备。利用RMON功能，网管可以快速跟踪网络、网段或设备出现的故障，积极采取防范措施，防止网络资源的失效，同时RMON MIB也可以记录网络性能和故障的数据，您可以在任何时候访问历史数据从而进行有效的故障诊断。RMON减少了SNMP管理者同代理间的通信流量，使得网管可以简单而有效地管理大型网络。

➢ **RMON 的工作原理**

RMON 代理在 RMON MIB 中存储网络信息，交换机置入 RMON 代理后，具有了 RMON 探测的功能。管理者使用 SNMP 的基本命令与 RMON 代理交互数据信息，收集网络管理信息。但是由于设备资源的限制，管理者无法获取 RMON MIB 的全部数据，一般只可以收集到四个组的信息，这四个组是：历史组、事件组、统计组和警报组。

➢ **RMON 组**

本交换机支持 RMON 规范（RFC1757）中定义的历史组、事件组、统计组和警报组。

RMON 组	功能	元素
历史组	周期性地收集网络统计信息，存储起来以便日后提取，从而有效的监测网络。	采样端口、采用间隔、创建者。
事件组	定义事件序号及事件的处理方式。此处定义的事件主要用在警报组中警报触发产生的事件。	事件描述、事件类型、创建者、用户名。
统计组	监测报警变量在指定端口的统计值。	丢弃数据包、丢弃字节、数据包发送、广播数据包、组播数据包、CRC 错误帧、过小（或超大）的数据报文、冲突帧以及计数器的数据包。范围从 64、65~127、128~255、256~511、512~1023 以及 1024~10240 字节。

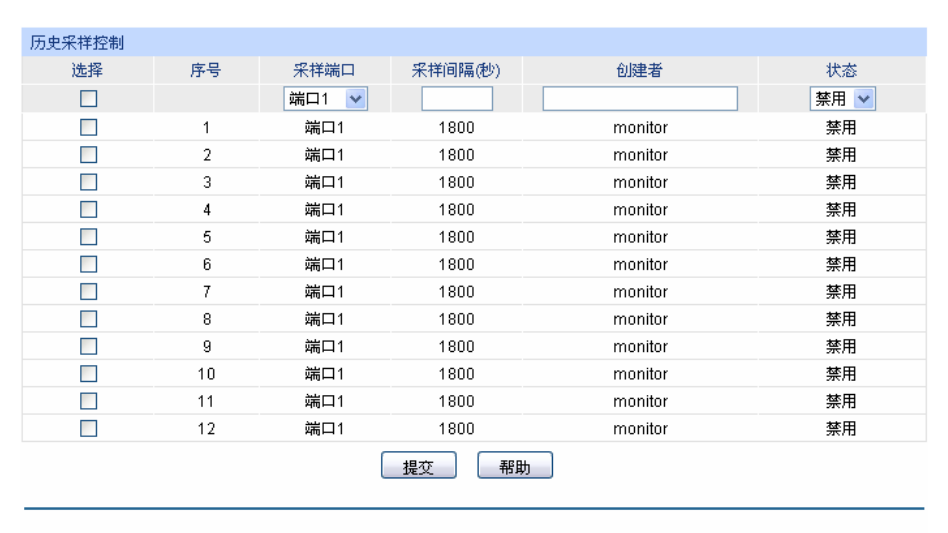
警报组	定期对指定的警报变量进行监测，一旦计数器超过阈值则触发警报。	警报变量、样例类型、时间间隔、阈值上限、阈值下限、警报触发方式。

在本功能处可以配置 RMON 的各个组，包括**历史采样**、**事件配置**和**警报管理**三个配置页面。

12.3.1 历史采样

本页用来配置 RMON 的历史组。

进入页面的方法：**SNMP>>RMON>>历史采样**



历史采样控制

选择	序号	采样端口	采样间隔(秒)	创建者	状态
☐		端口1			禁用
☐	1	端口1	1800	monitor	禁用
☐	2	端口1	1800	monitor	禁用
☐	3	端口1	1800	monitor	禁用
☐	4	端口1	1800	monitor	禁用
☐	5	端口1	1800	monitor	禁用
☐	6	端口1	1800	monitor	禁用
☐	7	端口1	1800	monitor	禁用
☐	8	端口1	1800	monitor	禁用
☐	9	端口1	1800	monitor	禁用
☐	10	端口1	1800	monitor	禁用
☐	11	端口1	1800	monitor	禁用
☐	12	端口1	1800	monitor	禁用

提交 帮助

图 12-9 历史采样

条目介绍：

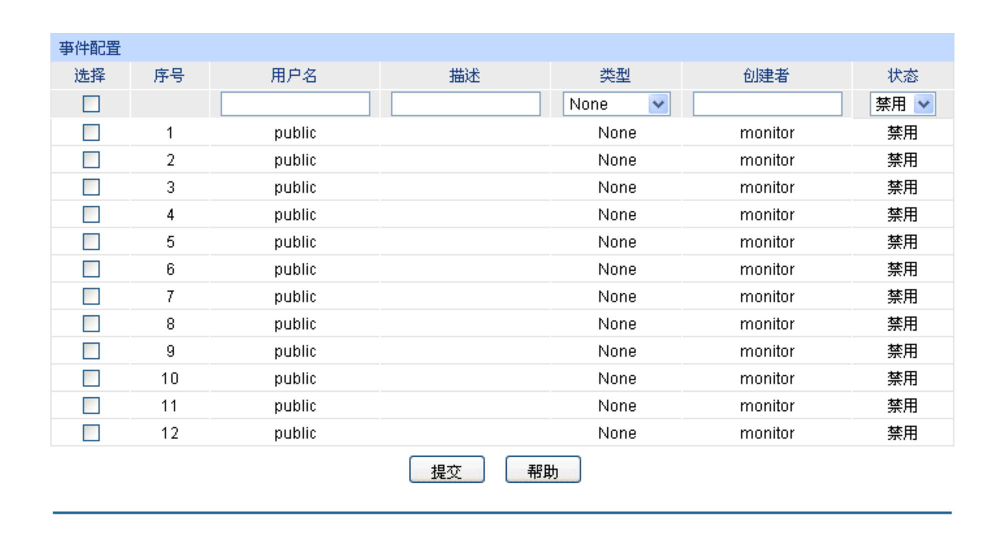
➤ 历史采样控制

选择：	勾选条目配置采样属性。
序号：	显示采样条目的序号。
采样端口：	选择进行采样的端口。
采样间隔：	填写端口采样的时间间隔。默认为 1800 秒。
创建者：	填写创建该采样条目的实体。
状态：	选择是否启用所选采样条目。

12.3.2 事件配置

本页用来配置 RMON 的事件组。

进入页面的方法：**SNMP>>RMON>>事件配置**



事件配置

选择	序号	用户名	描述	类型	创建者	状态
☐				None		禁用
☐	1	public		None	monitor	禁用
☐	2	public		None	monitor	禁用
☐	3	public		None	monitor	禁用
☐	4	public		None	monitor	禁用
☐	5	public		None	monitor	禁用
☐	6	public		None	monitor	禁用
☐	7	public		None	monitor	禁用
☐	8	public		None	monitor	禁用
☐	9	public		None	monitor	禁用
☐	10	public		None	monitor	禁用
☐	11	public		None	monitor	禁用
☐	12	public		None	monitor	禁用

提交 帮助

图 12-10 事件配置

条目介绍：

➢ 事件配置

选择： 勾选条目配置事件属性。

序号： 显示事件条目的序号。

用户名： 填写事件所属的用户。当对应事件需要发送通知时，将会根据此用户名进行发送。

描述： 填写该事件的描述信息。

类型： 选择事件的类型。

- None：不做任何操作。
- 日志：将事件记录在交换机中，通过 SNMP 管理软件读取。
- 通知：向管理主机发送报警消息。
- 日志&通知：将事件记录在交换机中并向管理主机发送报警消息。

创建者： 填写创建该事件条目的实体。

状态： 选择是否启用所选事件条目。

12.3.3 警报管理

本页用来配置 RMON 的统计组和警报组。

进入页面的方法：**SNMP>>RMON>>警报管理**



警报配置

选择	序号	计数器	端口	样例类型	上升阈值	上升事件	下降阈值	下降事件	启动警报	时间间隔(秒)	创建者	状态
☐		DropEvent		绝对值					全部			禁用
☐	1	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用
☐	2	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用
☐	3	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用
☐	4	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用
☐	5	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用
☐	6	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用
☐	7	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用
☐	8	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用
☐	9	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用
☐	10	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用
☐	11	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用
☐	12	DropEvent	端口1	绝对值	100	0	100	0	全部	1800	monitor	禁用

提交 帮助

图 12-11 警报配置

条目介绍：

➢ **事件配置**

选择：	勾选条目配置警报属性。
序号：	显示警报条目的序号。
计数器：	选择警报变量。
端口：	选择进行警报监视的端口号。
样例类型：	为警报变量选择取样的方法，再将取样的值与阈值进行比较。 ● 绝对值：在一个取样周期结束时将取样结果与阈值进行比较。 ● 增量：将现在值减去上一次取样值之后的增量与阈值进行比较。
上升阈值：	填写触发警报的上升阈值。默认为 100。
上升事件：	选择触发上升阈值警报的事件的序号。
下降阈值：	填写触发警报的下降阈值。默认为 100。
下降事件：	选择触发下降阈值警报的事件的序号。
启动警报：	选择警报触发的方式。 ● 上升：只在触发上升阈值后触发警报。 ● 下降：只在触发下降阈值后触发警报。 ● 全部：触发上升和下降阈值均触发警报。
时间间隔：	填写警报的时间间隔。默认为 1800 秒。
创建者：	填写创建该警报条目的实体。
状态：	选择是否启用所选警报条目。



注意：

- 当警报变量的采样值在同一方向上连续多次超过阈值时，只会在第一次产生警报事件。即上升警报和下降警报是交替产生的，出现了一次上升警报，则下一次必为下降警报。

回目录

第13章 集群管理

随着网络技术的发展，网络的规模越来越大，网络设备的数量越来越多，所以网络管理也就越来越烦琐。数量众多的设备需要分配不同的网络地址，每台管理设备均需要单独配置之后才能够满足应用的需要，以上这些造成管理人员很大的压力。

集群管理可以很好地解决上述问题。集群是可以当作单一设备来管理的一组网络设备的集合，集群管理的主要目的是解决大量分散的网络设备的集中管理问题。网络管理者通过集群中的一个交换机就可以实现对集群中其他交换机的管理和维护；其中执行管理功能的交换机是命令交换机，其他被管理的交换机是成员交换机，命令交换机和成员交换机组成了一个“集群”。典型组网应用如图 13-1 所示。

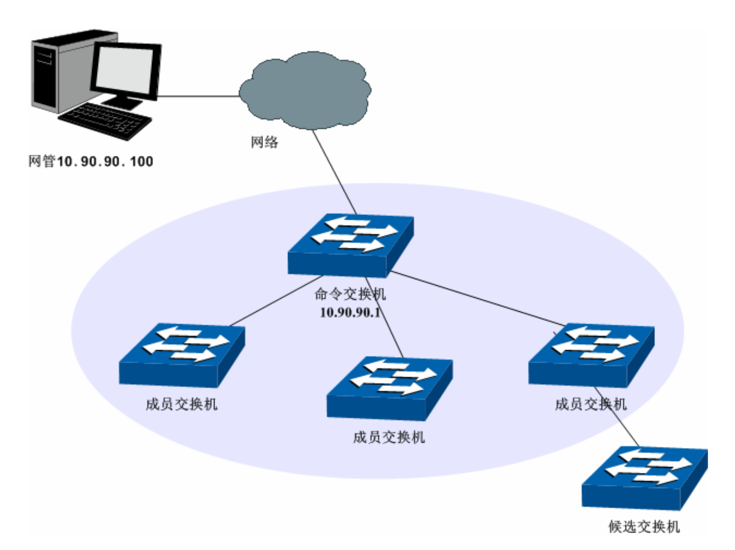


图 13-1 集群典型应用组网图

➢ **集群角色**

由于各个交换机在集群中所处的地位和功能的不同，形成了不同的角色，您可以配置交换机在集群中的角色。集群的角色有三种：

命令交换机：在集群中，唯一的可以配置和管理整个集群的交换机。命令交换机通过收集 NDP（Neighbor Discovery Protocol，邻居发现协议）和 NTDP（Neighbor Topology Discovery Protocol，邻居拓扑发现协议）信息来发现和确定候选交换机。

成员交换机：集群中被管理的交换机。

候选交换机：具有加入集群能力，但还没有加入任何集群的交换机。

独立交换机：未启用集群功能的交换机。

各种集群角色可以按一定的规则进行转换：

- 用户在交换机上创建集群的同时，将当前交换机指定为命令交换机。
- 命令交换机通过收集相关信息，发现和确定候选交换机。
- 候选交换机加入集群后，成为成员交换机。
- 集群内的成员交换机被删除后将恢复为候选交换机。
- 命令交换机只有在删除集群时才能恢复为候选交换机。

➢ 集群工作原理

集群通过 NDP、NTDP、CMP（Cluster Management Protocol，集群管理协议）三个协议，对集群内部的交换机进行配置和管理。

集群的过程分为拓扑发现、拓扑收集和集群的建立维护，具体工作过程如下：

- 拓扑发现：所有交换机通过 NDP 来获取邻居交换机的信息。
- 拓扑收集：命令交换机通过 NTDP 来收集网络内指定跳数范围内的交换机信息以及各个交换机的连接信息，并从收集到的拓扑信息中确定集群的候选交换机。
- 集群建立维护：命令交换机根据 NTDP 收集到的候选设备信息完成将候选交换机加入集群、成员交换机离开集群等集群管理操作。

集群管理模块主要用于配置交换机的集群管理功能，包括**拓扑发现**、**拓扑收集**以及**集群管理**三个部分。

13.1 拓扑发现

集群中的交换机使用 NDP 来获取与其直接相连的邻居交换机的信息。交换机周期性地向邻居发送 NDP 报文，同时也会接收但不转发邻居交换机发送的 NDP 报文。NDP 报文中包含 NDP 信息（包括本交换机的名称、MAC 地址、软件版本等信息）等。

交换机会存储和维护一个邻居信息表，邻居信息表里包含每个邻居交换机的 NDP 信息表项。如果交换机收到新邻居的 NDP 信息，则会在邻居信息表新增一个表项；如果从邻居交换机收到的 NDP 信息与旧的信息不同，则更新邻居信息表中的数据，如果相同，则只更新老化时间，如果超过老化时间还没有收到邻居发送的 NDP 信息，将自动删除相应的邻居表项。

本功能包括**邻居信息**、**配置显示**和**全局配置**三个配置页面。

13.1.1 邻居信息

在本页可以查看交换机的 NDP 邻居信息表。

进入页面的方法：集群管理>>拓扑发现>>邻居信息



图 13-2 邻居信息

条目介绍：

➢ 邻居查找

查找选项： 选择欲查找条目需包含的信息。

➤ 邻居信息

本地端口： 显示本交换机的端口号。

远程端口： 显示与相应端口相连的邻居交换机的端口号。

设备名称： 显示邻居交换机的名称。

设备 MAC： 显示邻居交换机的 MAC 地址。

软件版本： 显示邻居交换机的软件版本。

老化时间： 显示邻居交换机发送的 NDP 报文在本交换机上的剩余时间。

13.1.2 配置显示

在本页可以查看交换机的 NDP 配置信息。

进入页面的方法：**集群管理>>拓扑发现>>配置显示**

全局配置

NDP状态： 启用

老化定时器： 180秒

Hello定时器： 60秒

端口状态

端口	NDP状态	发送NDP包数	接收NDP包数	错误NDP包数	邻居数	详细信息
1	启用	0	0	0	0	详细信息
2	启用	164	585	0	5	详细信息
3	启用	0	0	0	0	详细信息
4	启用	0	0	0	0	详细信息
5	启用	0	0	0	0	详细信息
6	启用	0	0	0	0	详细信息
7	启用	0	0	0	0	详细信息
8	启用	0	0	0	0	详细信息
9	启用	0	0	0	0	详细信息
10	启用	165	0	0	0	详细信息
11	启用	0	0	0	0	详细信息
12	启用	0	0	0	0	详细信息

刷新 帮助

图 13-3 配置显示

条目介绍：

➤ 全局配置

NDP 状态： 显示本交换机的全局 NDP 状态。

老化定时器： 显示本交换机发送的 NDP 报文在邻居交换机上的老化时间。

Hello 定时器： 显示本交换机 NDP 报文发送的间隔时间。

➢ 端口状态

端口： 显示交换机的端口号。

NDP 状态： 显示当前端口的 NDP 状态。

发送 NDP 包数： 显示端口当前发送的 NDP 数据包数。

接收 NDP 包数： 显示端口当前接收的 NDP 数据包数。

错误 NDP 包数： 显示端口当前接收到的错误 NDP 数据包数。

邻居数： 显示端口所连接的邻居交换机数。

详细信息： 点击此按键，将显示该端口的收集到的邻居信息。

13.1.3 全局配置

在本页可以配置交换机的 NDP 功能。

进入页面的方法：集群管理>>拓扑发现>>全局配置

全局配置

NDP状态： ◉ 启用 ○ 禁用

老化定时器： 180 秒（5-255，默认为180） 提交

Hello定时器： 60 秒（5-254，默认为60）

端口状态

选择	端口	NDP状态	选择	端口	NDP状态
☐	1	启用	☐	2	启用
☐	3	启用	☐	4	启用
☐	5	启用	☐	6	启用
☐	7	启用	☐	8	启用
☐	9	启用	☐	10	启用
☐	11	启用	☐	12	启用
☐	13	启用	☐	14	启用
☐	15	启用	☐	16	启用
☐	17	启用	☐	18	启用
☐	19	启用	☐	20	启用
☐	21	启用	☐	22	启用
☐	23	启用	☐	24	启用
☐	25	启用	☐	26	启用
☐	27	启用	☐	28	启用

全选 启用 禁用 帮助

图 13-4 全局配置

条目介绍：

➢ 全局配置

NDP 状态： 选择是否启用全局 NDP 功能。

老化定时器： 填写本交换机发送的 NDP 报文在接收设备上的老化时间。默认为 180 秒。

Hello 定时器： 填写本交换机 NDP 报文发送的时间间隔。默认为 60 秒。

➢ 端口状态

选择： 勾选端口配置端口 NDP 状态。

端口： 显示交换机的端口号。

NDP 状态： 显示端口当前的 NDP 状态。

启用： 点击后启用所选端口的 NDP 功能。

禁用： 点击后禁用所选端口的 NDP 功能。

注意：

- 必须在全局配置和端口状态中同时启用 NDP 状态，NDP 功能才能正常运行。
- 老化定时器时间要大于 Hello 定时器时间，否则将引起 NDP 端口邻居信息表的不稳定。

13.2 拓扑收集

NTDP 用于命令交换机收集整个网络指定跳数的拓扑信息。NTDP 根据 NDP 邻居信息表发送和转发 NTDP 拓扑收集请求，收集指定跳数内的网络中每个交换机的 NDP 信息及其连接信息。命令交换机可以定时在网络内进行拓扑收集，您也可以随时在命令交换机上手动启用拓扑收集。

命令交换机发送拓扑收集请求报文后，大量交换机会同时收到拓扑收集请求并同时发送拓扑收集响应报文，如此以来可能造成网络拥塞和命令交换机负担过重。为了避免上述现象的产生，设计了两个时间参数来控制拓扑收集请求报文扩散速度：

- 请求跳数延迟时间：交换机收到拓扑收集请求，会等待该时间段之后，才开始在第一个启用 NTDP 的端口转发该拓扑收集请求报文。
- 端口跳数延迟时间：在同一个交换机上，除第一个端口外，每个启用 NTDP 功能的端口在前一个端口发送拓扑收集请求报文后，都会等待该时间段，再进行拓扑收集请求报文的转发。

本功能包括**设备列表**、**配置显示**和**全局配置**三个配置页面。

13.2.1 设备列表

在此处可以查看 NTDP 收集到的设备信息。同时，无论集群是否建立，您都可以在本页随时手动收集 NTDP 信息，从而更有效地对设备进行实时管理与监控。

进入页面的方法：集群管理>>拓扑收集>>设备列表



设备信息列表

设备类型	设备MAC	集群名	角色	跳数	邻居信息
TL-SL5428 1.0	00-3C-95-1D-DF-1F		候选交换机	1	详细信息
TL-SL5428 1.0	00-21-8C-EA-4E-D3		候选交换机	0	详细信息

拓扑收集　刷新　帮助

图 13-5 设备列表

条目介绍：

➤ 设备信息列表

设备类型： 显示 NTDP 所收集到的设备信息。

设备 MAC： 显示该设备的 MAC 地址。

集群名： 显示该设备的集群名称。

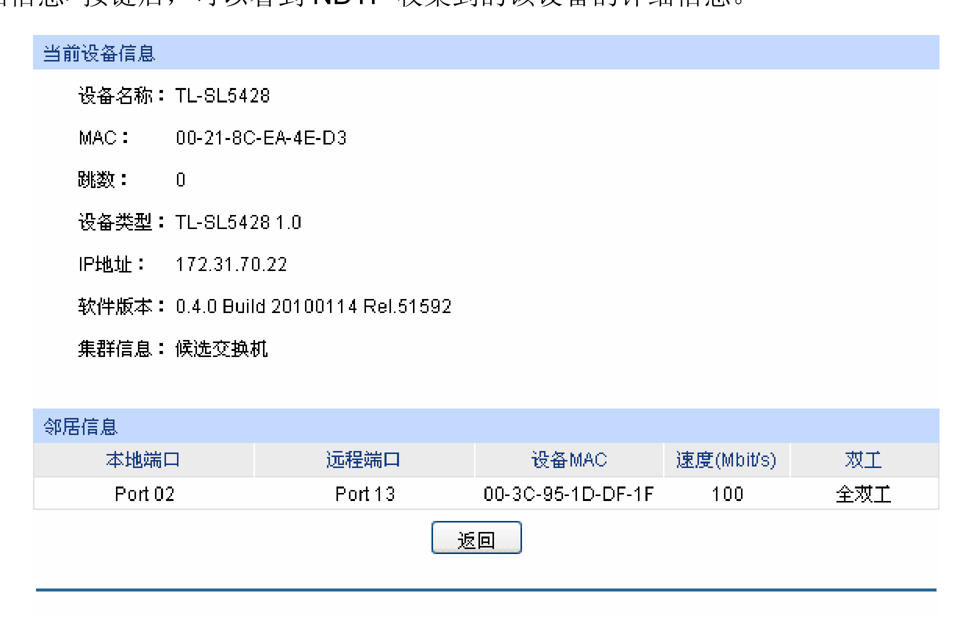
角色： 显示该设备在集群中的角色。

- 命令交换机：配置并管理集群的交换机。
- 成员交换机：在集群中被管理的交换机。
- 候选交换机：能够成为集群成员但是还未加入集群的交换机。
- 独立交换机：未启用集群功能的交换机。

跳数： 显示该设备距离本交换机的跳数。

邻居信息： 点击<详细信息>，可以查看该设备的详细信息及其邻居信息表。

点击<详细信息>按键后，可以看到 NDTP 收集到的该设备的详细信息。



当前设备信息

设备名称：TL-SL5428
MAC： 00-21-8C-EA-4E-D3
跳数： 0
设备类型：TL-SL5428 1.0
IP地址： 172.31.70.22
软件版本：0.4.0 Build 20100114 Rel.51592
集群信息：候选交换机

邻居信息

本地端口	远程端口	设备MAC	速度(Mbit/s)	双工
Port 02	Port 13	00-3C-95-1D-DF-1F	100	全双工

返回

图 13-6 当前设备信息

13.2.2 配置显示

在本页可以查看交换机的 NTDP 配置信息。

进入页面的方法：集群管理>>拓扑收集>>配置显示

全局配置

NTDP状态：	启用
拓扑收集间隔时间：	1分钟
拓扑收集跳数：	3跳
请求跳数延迟时间：	200毫秒
端口跳数延迟时间：	20毫秒

端口状态

端口	NTDP状态	端口	NTDP状态
1	启用	2	启用
3	启用	4	启用
5	启用	6	启用
7	启用	8	启用
9	启用	10	启用
11	启用	12	启用
13	启用	14	启用
15	启用	16	启用
17	启用	18	启用
19	启用	20	启用
21	启用	22	启用
23	启用	24	启用
25	启用	26	启用
27	启用	28	启用

刷新 帮助

图 13-7 配置显示

条目介绍：

➢ 全局配置

NTDP 状态： 显示本交换机的全局 NTDP 状态。

拓扑收集间隔时间： 显示本交换机拓扑信息收集的周期。

拓扑收集跳数： 显示本交换机拓扑收集的范围。

请求跳数延迟时间： 显示本交换机在收到拓扑请求报文到第一次转发拓扑请求报文的延时时间。

端口跳数延迟时间： 显示本交换机在相邻端口转发拓扑请求报文的延时时间。

➢ 端口状态

端口： 显示交换机的端口号。

NTDP 状态： 显示当前端口的 NTDP 状态。

13.2.3 全局配置

在本页可以配置交换机的 NTDP 功能。

进入页面的方法：集群管理>>拓扑发现>>全局配置

全局配置

NTDP状态：	◉ 启用 ○ 禁用	
拓扑收集间隔时间：	1	分钟（1-60，默认为1）
拓扑收集跳数：	3	跳（1-16，默认为3） 提交
请求跳数延迟时间：	200	毫秒（1-1000，默认为200）
端口跳数延迟时间：	20	毫秒（1-100，默认为20）

端口状态

选择	端口	NTDP状态	选择	端口	NTDP状态
☐	1	启用	☐	2	启用
☐	3	启用	☐	4	启用
☐	5	启用	☐	6	启用
☐	7	启用	☐	8	启用
☐	9	启用	☐	10	启用
☐	11	启用	☐	12	启用
☐	13	启用	☐	14	启用
☐	15	启用	☐	16	启用
☐	17	启用	☐	18	启用
☐	19	启用	☐	20	启用
☐	21	启用	☐	22	启用
☐	23	启用	☐	24	启用
☐	25	启用	☐	26	启用
☐	27	启用	☐	28	启用

全选 启用 禁用 帮助

图 13-8 全局配置

条目介绍：

➢ 全局配置

NTDP 状态： 选择是否启用全局 NTDP 功能。

拓扑收集间隔时间： 填写本交换机拓扑信息收集的周期。默认为 1 分钟。

拓扑收集跳数： 填写本交换机拓扑收集的范围。默认为 3 跳。

请求跳数延迟时间： 填写本交换机在收到拓扑请求报文到第一次转发拓扑请求报文的延时时间。默认为 200 毫秒。

端口跳数延迟时间： 填写本交换机在相邻端口转发拓扑请求报文的延时时间。默认为 20 毫秒。

➢ 端口状态

选择： 勾选端口配置端口 NTDP 状态。

端口： 显示交换机的端口号。

NTDP 状态： 显示端口当前的 NTDP 状态。

启用： 点击后启用所选端口的 NTDP 功能。

禁用： 点击后禁用所选端口的 NTDP 功能。



- 必须在全局配置和端口状态中同时启用 NTDP 状态，NTDP 功能才能正常运行。

13.3 集群管理

命令交换机通过 NDP 和 NTDP 协议发现和确定候选交换机，并将候选交换机自动加入集群，您也可以通过手动配置将候选交换机加入到集群中。候选交换机成功加入集群后，将获得由命令交换机为它分配的私有 IP 地址。您可以在命令交换机上直接访问成员交换机的 Web 页面，对成员交换机进行管理。

本功能包括**配置显示**、**集群配置**、**成员管理**和**拓扑图**四个配置页面。

13.3.1 配置显示

在本页可以查看到当前集群的状态。

进入页面的方法：集群管理>>集群管理>>配置显示

- 当前交换机为候选交换机时，可以看到：

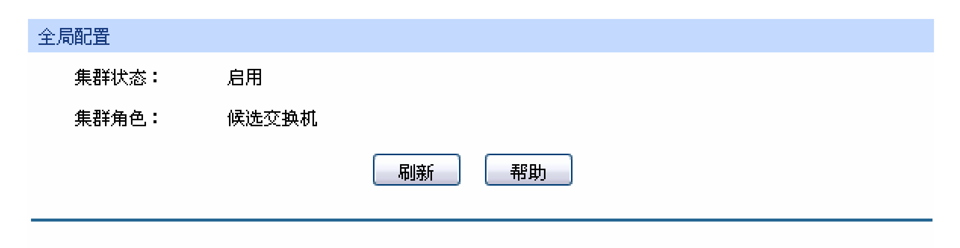


图 13-9 候选交换机的配置显示

条目介绍：

➢ 全局配置

集群状态： 显示当前交换机的集群状态。

集群角色： 显示交换机在集群中的角色。

- 当前交换机为命令交换机时，可以看到



图 13-10 命令交换机的配置显示

条目介绍：

➢ 全局配置

集群状态： 显示当前交换机的集群状态。

集群角色： 显示交换机在集群中的角色。

集群名： 显示交换机当前的集群名称。

➢ 集群设置

集群地址池、掩码： 显示集群中成员交换机的私有 IP 地址范围。

保持时间： 显示集群信息在命令交换机中保存的时间。

时间间隔： 显示本交换机与成员交换机握手报文的时间间隔。

➢ 成员信息

设备名称： 显示成员交换机的名称。

设备 MAC： 显示成员交换机的 MAC 地址。

IP 地址： 显示成员交换机在集群中的 IP 地址。

状态： 显示成员交换机的连通性。

角色： 显示交换机当前的集群角色。

加入集群时间： 显示成员交换机加入集群的时间。

跳数： 显示成员交换机距离命令交换机的跳数。

● 当前交换机为成员交换机时，可以看到：

全局配置

集群状态： 启用

集群角色： 成员交换机

集群名： hello

命令交换机MAC： 00-02-03-BA-24-8D

刷新 帮助

图 13-11 成员交换机的配置显示

条目介绍：

➢ 全局配置

集群状态： 显示当前交换机的集群状态。

集群角色： 显示交换机在集群中的角色。

集群名： 显示交换机当前的集群名称。

命令交换机 MAC： 显示命令交换机的 MAC 地址。

● 当前交换机为独立交换机时，可以看到：

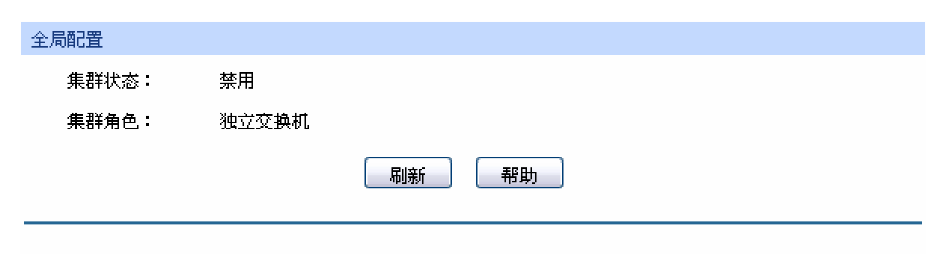


图 13-12 独立交换机的配置显示

条目介绍：

➢ 全局配置

集群状态： 显示当前交换机的集群状态。

集群角色： 显示交换机在集群中的角色。

13.3.2 集群配置

在本页可以配置交换机的集群状态。

进入页面的方法：集群管理>>集群管理>>集群配置

● 当前交换机为候选交换机时，可以看到：

当前角色

集群角色： 候选交换机

角色转换

集群角色转换： 独立交换机 命令交换机

集群名： （1-16个字符）

集群地址池： 掩码：

提交 帮助

图 13-13 候选交换机的集群配置

条目介绍：

➢ 当前角色

集群角色： 显示交换机在集群中的角色。

➢ 角色转换

独立交换机： 将交换机的集群角色转换为独立交换机。

命令交换机： 将交换机的集群角色转换为命令交换机。之后，您还需要配置集群的基本属性：

- 集群名：配置交换机当前的集群名称。
- 集群地址池、掩码：配置集群中成员交换机的私有 IP 地址范围。

- 当前交换机为命令交换机时，可以看到：

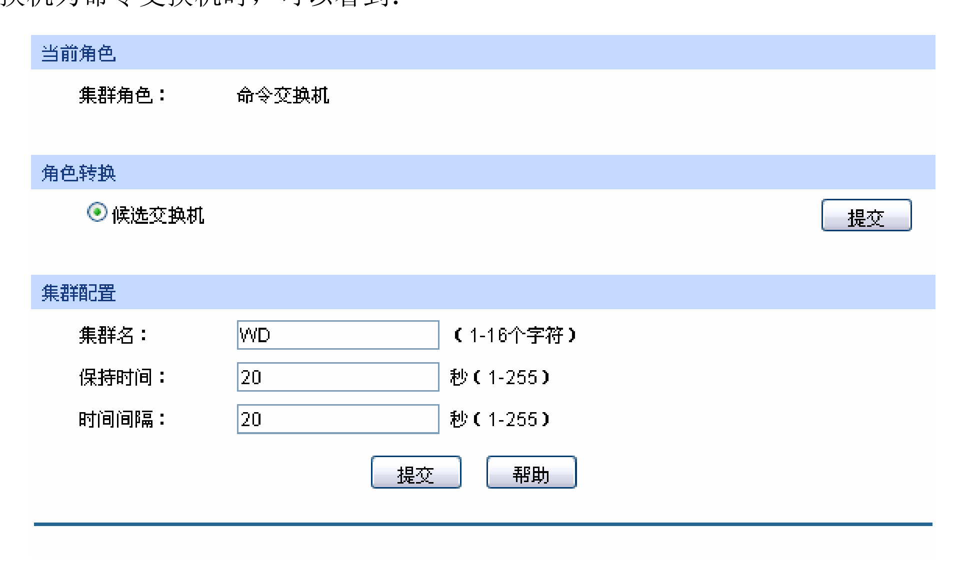


图 13-14 命令交换机的集群配置

条目介绍：

➢ 当前角色

集群角色： 显示交换机在集群中的角色。

➢ 角色转换

候选交换机： 将交换机的集群角色转换为候选交换机。

➢ 集群配置

集群名： 填写集群名称。

保持时间： 填写集群信息在命令交换机中保存的时间。

时间间隔： 填写命令交换机与成员交换机握手报文的时间间隔。

● 当前交换机为成员交换机时，可以看到：

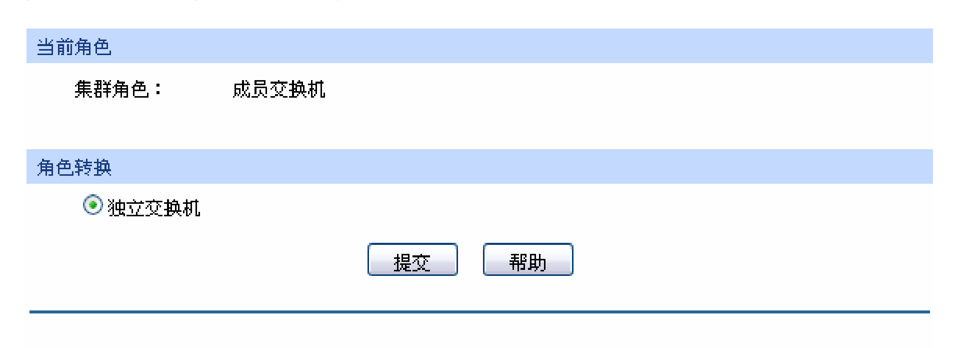


图 13-15 成员交换机的集群配置

条目介绍：

➢ 当前角色

集群角色： 显示交换机在集群中的角色。

➢ 角色转换

独立交换机： 将交换机的集群角色转换为独立交换机。

● 当前交换机为独立交换机时，可以看到：

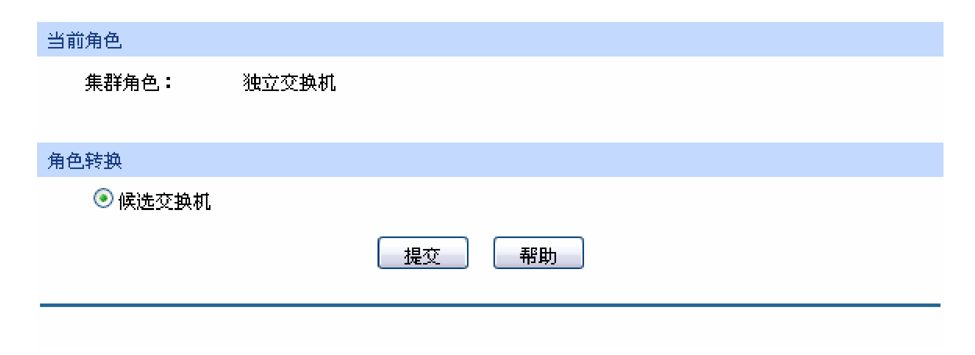


图 13-16 独立交换机的集群配置

条目介绍：

➤ 当前角色

集群角色： 显示交换机在集群中的角色。

➤ 角色转换

候选交换机： 将交换机的集群角色转换为候选交换机。

13.3.3 成员管理

当交换机为集群中的命令交换机时，可以在命令交换机上手动指定要加入集群的候选交换机，也可以手动删除集群中指定的成员交换机，同时也可以在本页对成员交换机进行配置管理。

进入页面的方法：集群管理>>集群管理>>成员管理



图 13-17 成员管理

条目介绍：

➤ 手动成员加入

成员 MAC： 填写候选交换机的 MAC 地址。

➤ 成员信息

选择： 勾选条目进行管理或删除操作。

设备名称： 显示成员交换机的名称。

设备 MAC： 显示成员交换机的 MAC 地址。

IP 地址： 显示成员交换机在集群中的 IP 地址。

状态： 显示成员交换机的连通性。

角色： 显示交换机当前的集群角色。

加入集群时间： 显示成员交换机加入集群的时间。

跳数： 显示成员交换机距离本交换机的跳数。

管理： 勾选条目后点击此按键，进入相应的成员交换机的 Web 页面。

13.3.4 拓扑图

在本页可以看到集群的整个拓扑结构图，也可以点击节点交换机直接进入相应的管理页面，从而对该交换机进行配置管理。同时双击拓扑图上的各个节点交换机，可以看到该交换机的详细信息。

进入页面的方法：**集群管理>>集群管理>>拓扑图**

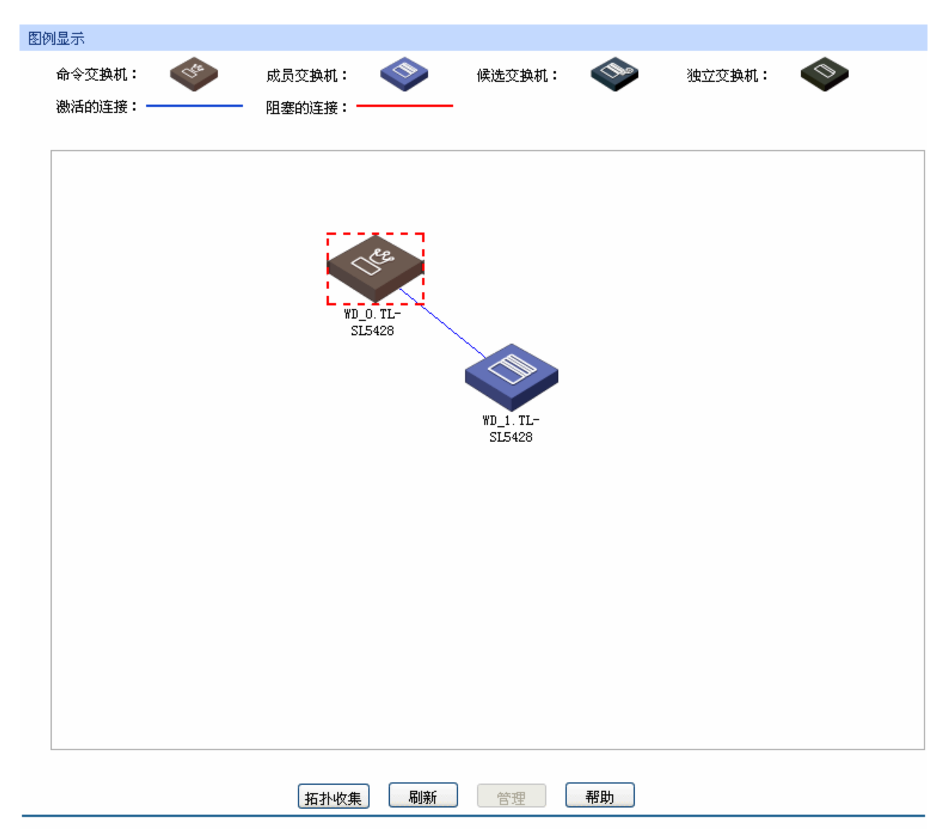


图 13-18 拓扑图

条目介绍：

➢ 图例显示

拓扑收集： 点击此按键后将集群内的拓扑信息以拓扑图的形式展现出来。

管理： 如果当前设备为集群中的命令交换机，并且选中的设备为此集群中的成员交换机，那么点击此按键，将进入相应交换机的管理页面。

集群管理功能全局配置步骤：

在配置集群之前，首先您需要明确集群内各交换机的角色及功能，做好集群的规划工作。

➢ 若此交换机为命令交换机。

步骤	操作	说明
1	启用系统和端口的 NDP 功能，并配置 NDP 参数	可选操作。在**集群管理>>拓扑发现>>全局配置**页面，启用交换机的 NDP 功能。

2	启用系统和端口的 NTDP 功能，并配置 NTDP 参数	可选操作。在**集群管理>>拓扑收集>>全局配置**页面，启用交换机的 NTDP 功能。
3	建立集群，并配置集群参数	可选操作。在**集群管理>>集群管理>>集群配置**页面，建立集群并配置集群参数。
4	管理集群设备	可选操作。 在**集群管理>>集群管理>>成员管理**页面，选择成员交换机，点击<管理>按键，即可进入该成员交换机的 Web 页面进行管理。 也可在**集群管理>>集群管理>>拓扑图**页面，双击交换机图标，可以查看该交换机的详细信息；单击交换机的图标，点击<管理>按键，即可进入该成员交换机的 Web 页面进行管理。

➢ 若此交换机为成员交换机。

步骤	**操作**	**说明**
1	启用系统和端口的 NDP 功能	可选操作。在**集群管理>>拓扑发现>>全局配置**页面，启用交换机的 NDP 功能。
2	启用系统和端口的 NTDP 功能	可选操作。在**集群管理>>拓扑收集>>全局配置**页面，启用交换机的 NTDP 功能。
3	手动收集拓扑信息	可选操作。 在**集群管理>>拓扑收集>>设备列表**页面，点击<拓扑收集>按键，手动收集拓扑信息。 也可在**集群管理>>集群管理>>拓扑图**页面，点击<拓扑收集>按键，手动收集拓扑信息。
4	查询集群中其它交换机的详细信息	在**集群管理>>集群管理>>拓扑图**页面，双击交换机图标，可以查看该交换机的详细信息。

13.4 集群管理功能组网应用

➢ 组网需求

三台交换机构成一个集群，其中：一台为命令交换机（以我司交换机 TL-SL5428 为例）、其它交换机为成员交换机（以我司交换机 TL-SL3428 为例）。网管通过命令交换机来管理整个集群。

- 命令交换机的端口 1 与外网连接，端口 2、端口 3 分别与成员交换机 1、成员交换机 2 连接。
- 集群地址池：175.128.0.1；掩码：255.255.255.0 。

➢ 组网图

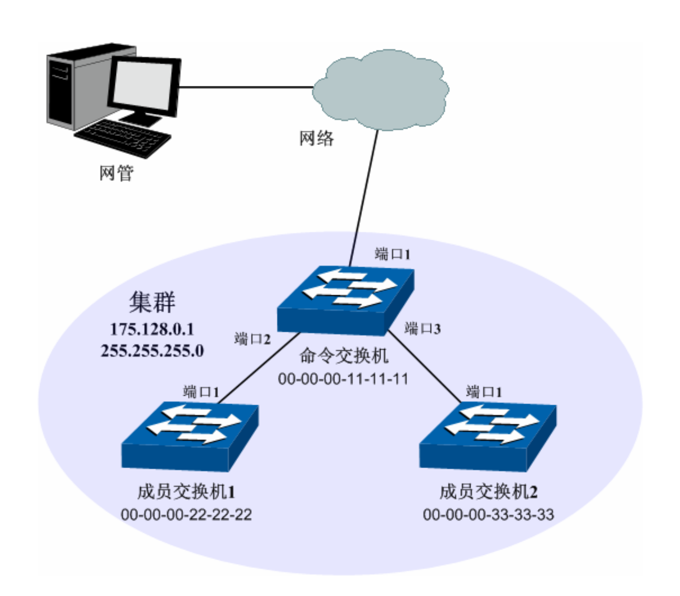


图 13-19 集群管理组网图

➢ **配置步骤**

● 配置成员交换机

步骤	操作	说明
1	启用系统和端口 1 的 NDP 功能	在**集群管理>>拓扑发现>>全局配置**页面，启用交换机的 NDP 功能。
2	启用系统和端口 1 的 NTDP 功能	在**集群管理>>拓扑收集>>全局配置**页面，启用交换机的 NTDP 功能。

● 配置命令交换机

步骤	操作	说明
1	启用系统和端口 1、2、3 的 NDP 功能	在**集群管理>>拓扑发现>>全局配置**页面，启用交换机的 NDP 功能。
2	启用系统和端口 1、2、3 的 NTDP 功能	在**集群管理>>拓扑收集>>全局配置**页面，启用交换机的 NTDP 功能。
3	建立集群，并配置集群参数	在**集群管理>>集群管理>>集群配置**页面，配置集群角色为命令交换机，并填写集群信息。 集群地址池：175.128.0.1 掩码：255.255.255.0
4	配置成员交换机	在**集群管理>>集群管理>>成员管理**页面，选择成员交换机，点击<管理>按键，进入该交换机的 Web 页面。 也可在**集群管理>>集群管理>>拓扑图**页面，双击交换机图标，可以查看该交换机的详细信息；单击交换机图标，点击<管理>按键，可以进入该交换机的 Web 页面。

回目录

第14章 系统维护

系统维护模块将管理交换机的常用系统工具组合在一起，为定位并排除交换机和网络故障提供便捷的方法。

1) 运行状态：对交换机内存和 CPU 进行监控。
2) 系统日志：通过系统日志查看在交换机上的配置参数并找出错误的配置。
3) 线缆检测：检测与交换机连接的线缆是否有故障。
4) 环回检测：检测本端设备与对端设备的可用性。
5) 网络诊断：检测目标是否可达以及目标与交换机之间的路由跳数。

14.1 运行状态

在本功能中可以通过曲线数据监控交换机 CPU 和内存的使用情况，CPU 和内存使用率应该在一定数值上下波动。当 CPU 和内存使用率波动较大且明显增大时，请检查网络是否受到攻击。

本功能包括 **CPU 监控**和**内存监控**两个配置页面。

14.1.1 CPU监控

进入页面的方法：系统维护>>运行状态>>CPU 监控

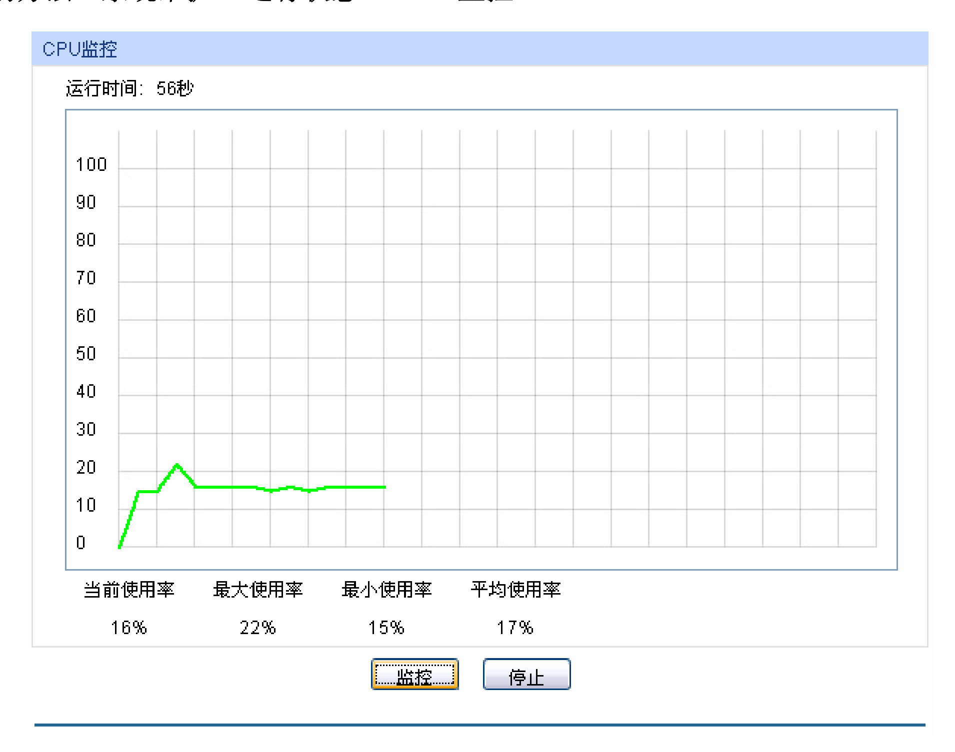


图14-1 CPU 监控

点击<监控>按键，图中会每隔 4 秒反馈一次监控数值，显示交换机 CPU 使用率。

14.1.2 内存监控

进入页面的方法：系统维护>>运行状态>>内存监控

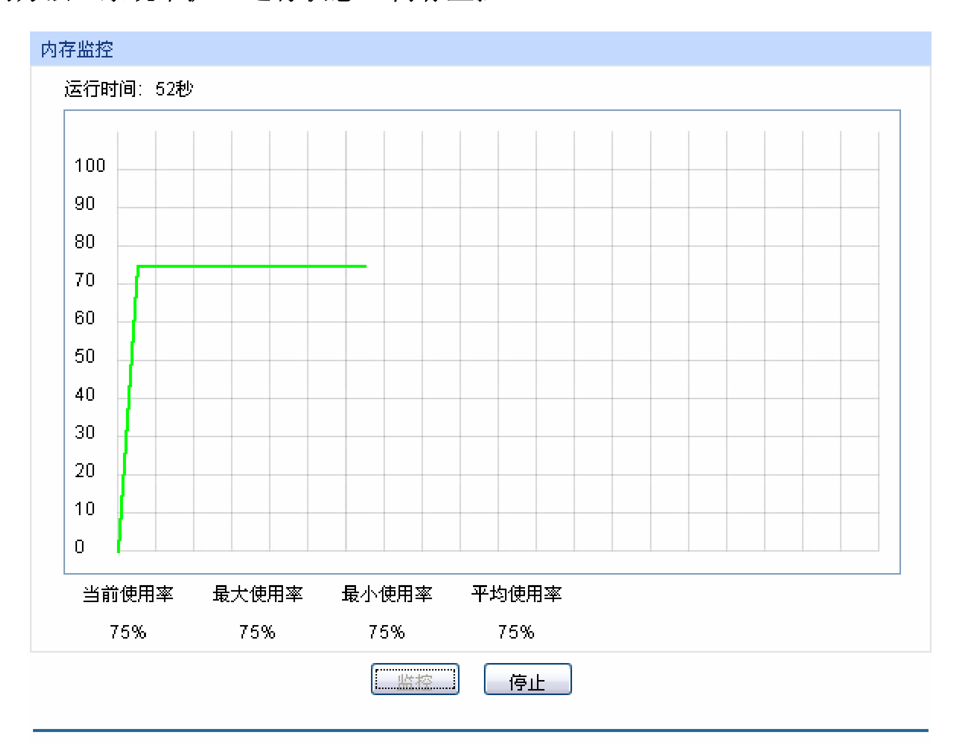


图14-2 内存监控

点击<监控>按键，图中会每隔 4 秒反馈一次监控数值，显示交换机内存使用率。

14.2 系统日志

本交换机提供的日志系统能够对所有的系统信息进行记载、分类、管理，为网络管理员监控设备运行情况和诊断设备故障提供强有力的支持。

本交换机的系统日志分为八个等级，如表14-1所示。

级别名称	等级	描述
emergencies	0	系统不可用信息
alerts	1	需要立刻做出反应的信息
critical	2	严重信息
errors	3	错误信息
warnings	4	警告信息
notifications	5	正常出现但是重要的信息
informational	6	需要记录的通知信息
debugging	7	调试过程产生的信息

表14-1 日志等级

本功能包括**日志列表**、**本地日志**、**远程日志**和**日志导出**四个功能页面。

14.2.1 日志列表

系统日志可以保存到两个不同的地方：日志缓冲区和日志文件。日志缓冲区的日志信息在交换机重启后将会丢失，日志文件里的日志信息在交换机重启后仍然有效。日志列表显示了日志缓冲区中的系统日志信息。

进入页面的方法：系统维护>>系统日志>>日志列表



系统日志列表

序号	时间	模块名	严重级别	日志信息
		所有模块	所有级别	
1	2006-01-01 08:00:03	LACP	level_5	LACP注册成功。
2	2006-01-01 08:00:03	QTable	level_5	DHCP监听初始化成功。
3	2006-01-01 08:00:03	QTable	level_5	DHCP监听消息类型注册成功。
4	2006-01-01 08:00:03	STP	level_5	MSTP模块CIST初始化成功。
5	2006-01-01 08:00:02	STP	level_5	MSTP模块消息类型注册成功。
6	2006-01-01 08:00:02	QTable	level_5	APR扫描初始化成功。
7	2006-01-01 08:00:02	QTable	level_5	APR扫描消息类型注册成功。
8	2006-01-01 08:00:02	GVRP	level_5	GVRP模块初始化成功。
9	2006-01-01 08:00:02	SNMP	level_5	SNMP初始化成功。
10	2006-01-01 08:00:01	QoS	level_5	QoS模块初始化成功。

刷新 帮助

注意：
1、严重级别划分为0-7共八个等级，级别值越小，紧急程度越高。
2、本页面显示记载在日志缓冲区中的日志信息，显示的条目数最多为512条。

图14-3 日志列表

条目介绍：

➢ 系统日志列表

序号：	显示该日志信息的序号。
时间：	显示该日志信息的发生时间。需先在**系统管理>>系统配置>>系统时间页面**进行配置后，系统日志才能获取到正确的时间。
模块名：	显示该日志信息所属功能模块，从下拉列表可选择显示某一模块的日志信息。
严重级别：	显示该日志信息的严重级别，从下拉列表选择某一级别，可显示小于或等于该级别值的日志信息。
日志信息：	显示该日志信息的内容。

注意：

- 严重级别划分为 0-7 共八个等级，级别值越小，紧急程度越高。
- 本页面显示记载在日志缓冲区中的日志信息，显示的条目数最多为 512 条。

14.2.2 本地日志

本地日志是指保存在本交换机上的所有系统日志信息。在缺省情况下，所有的系统日志将保存到日志缓冲区，而等级为 level_0 到 level_4 的系统日志将同时保存到日志文件中。在此页面中可以对日志的存储区进行配置。

进入页面的方法：系统维护>>系统日志>>本地日志

本地日志配置

选择	输出方向	严重级别	状态
☐			
☐	日志缓冲区	level_7	启用
☐	日志文件	level_4	启用

提交 帮助

注意：

1、本地日志包括日志缓冲区和日志文件两个输出方向。

2、严重级别划分为0-7共八个等级，级别值越小，紧急程度越高。

图14-4 本地日志

条目介绍：

➢ 系统日志列表

选择： 勾选相应的日志记录位置进行配置。

日志缓冲区： **日志列表**页面上显示的即为缓冲区中的信息，在断电重启后这些信息将会丢失。

日志文件： 日志文件中的日志信息在断电重启后不会丢失，可通过导出日志文件来查看。

严重级别： 限定各个输出方向上系统日志的严重级别。只有级别值小于或等于该值的系统日志才会进行记录。

状态： 启用/禁用保存到该位置的日志功能。

14.2.3 远程日志

远程日志功能可以将本交换机的系统日志发送到日志服务器上。日志服务器相当于一个可维护的共用消息区，它可以对网络中各设备产生的日志信息进行集中的监控和管理。

TP-LINK 日志服务器提供了一个用于日志监视、存储和管理的窗口系统，并提供自动备份的功能。日志格式遵循 RFC3164 标准，TP-LINK 日志服务器的安装过程及操作方法请登录我司官方网站 http://www.tp-link.com.cn 下载安装软件和操作指南。

进入页面的方法：**系统维护>>系统日志>>远程日志**

日志服务器

选择	序号	服务器IP	UDP端口号	严重级别	状态
☐					
☐	1	0.0.0.0	514	level_6	禁用
☐	2	0.0.0.0	514	level_6	禁用
☐	3	0.0.0.0	514	level_6	禁用
☐	4	0.0.0.0	514	level_6	禁用

提交 帮助

注意：

1、共支持4个日志服务器。

2、严重级别划分为0-7共八个等级，级别值越小，紧急程度越高。

图14-5 日志服务器

条目介绍：

➢ 日志服务器

选择：	勾选相应的日志服务器进行配置。
序号：	日志服务器序号。本交换机共支持 4 个日志服务器。
服务器 IP：	配置日志服务器的 IP 地址。
UDP 端口号：	发送/接收系统日志时所用到的 UDP 端口号，这里使用标准的 514 端口。
严重级别：	限定发往各个服务器上系统日志的严重级别。只有级别值小于或等于该值的系统日志才会发送到相应的服务器。
状态：	启用/禁用该服务器。

14.2.4 日志导出

日志导出功能可以将保存在交换机里的日志信息以文件的形式导出，作为设备诊断和统计分析之用。尤其在发生严重错误导致系统崩溃时，可在重启后导出日志信息，以获取相关的一些重要信息，为诊断设备提供支持。

进入页面的方法：系统维护>>系统日志>>日志导出

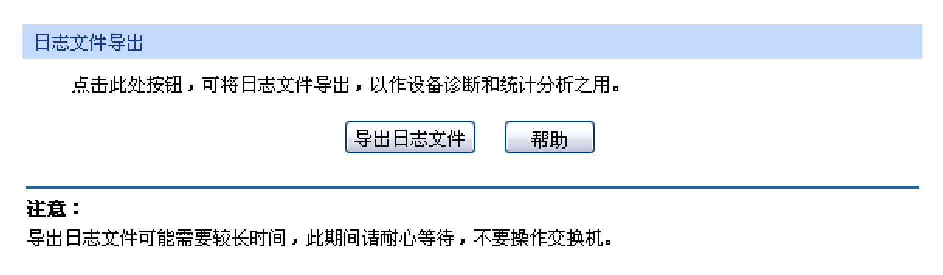


图14-6 日志导出

条目介绍：

➢ 日志文件导出

导出日志文件：	点击此按键导出日志文件中的日志信息。

14.3 系统诊断

本交换机提供了线缆检测和环回检测功能。

14.3.1 线缆检测

线缆检测功能能够检测与交换机相连的线缆是否有故障以及故障的位置，利用此功能可以辅助日常工程安装诊断。

进入页面的方法：系统维护>>系统诊断>>线缆检测



图14-7 线缆检测

条目介绍：

➢ 线缆检测

检测端口： 选择要进行线缆检测的端口。

线对： 显示线对序号。

线路状态： 检测端口连接的线缆的状态。可能显示的状态有：正常、短路、开路、阻抗失配。另外还可能出现线路不支持检测或检测失败的情况。

- 开路：线路中有断开现象，造成这种情况的原因一般是水晶头处线缆接触不良，可用线缆测试设备进行故障点定位。
- 短路：线路金属内芯互相接触，导致短路。
- 阻抗失配：网线质量问题。

线路长度： 若线路为正常状态，显示该线缆的长度范围。

出错长度： 若线路为短路、开路或阻抗失配状态，则显示该线缆的出错长度。

注意：

- 这里的长度是指线缆绕对的长度，不是线缆表皮的长度，线缆检测的长度可能存在误差。
- 检测结果仅供参考，特殊的情况也可能会检测错误或失败。

14.3.2 环回检测

环回检测可以在不依赖外部设备的情况下检查端口是否可用，同时可以检测对端设备的可用性，有助于确定和解决网络故障，能够迅速方便地定位网络故障。本交换机的环回检测分为内环检测和外环检测。

1) 内环检测：无须借助外部设备，即可检测交换机端口是否正常。

2) 外环检测：可以检测与交换机相连的对端设备是否正常，同时插入自环头进行还可以检测交换机的自身性能。自环头的做法是用网线将一个水晶头的 1/3、2/6、4/7、5/8 管脚成对短接即可。

进入页面的方法：系统维护>>系统诊断>>环回检测

检测类型

检测类型： ◉内环 ○外环

检测端口

☐1	☐2	☐3	☐4	☐5	☐6
☐7	☐8	☐9	☐10	☐11	☐12
☐13	☐14	☐15	☐16	☐17	☐18
☐19	☐20	☐21	☐22	☐23	☐24
☐25	☐26	☐27	☐28		

检测 帮助

检测结果

测试端口:无

测试类型:无

测试结果:无

图14-8 环回检测

条目介绍：

➢ 检测类型

检测类型： 选择要进行检测的类型。外环检测需要连接到外部设备或者自环头。

➢ 检测端口

检测端口： 勾选端口进行环回测试。

检测： 点击此按键进行检测。

14.4 网络诊断

本交换机提供了 Ping 检测和 Tracert 检测功能。

14.4.1 Ping检测

Ping 检测功能可以检测交换机与某网络设备是否可达，方便网络管理员检查网络的连通性，定位网络故障。

Ping 检测过程如下：

1) 交换机向目标设备发送 ICMP 请求报文；

2) 如果网络工作正常，则目标设备在接收到该报文后，向交换机返回 ICMP 应答报文；显示相关统计信息；

3) 如果网络工作异常，源设备将显示目的地址不可达或超时等提示信息。

进入页面的方法：**系统维护>>网络诊断>>Ping 检测**

Ping 检测

目标IP地址： 192.168.0.1

发送次数： 4 次（1-10）

发送报文长度： 64 字节（1-1024）

时间间隔： 100 毫秒（100-1000）

Ping

帮助

Ping 结果

Pinging 192.168.0.1 with 64 bytes of data :

Destination Host Unreachable!

Destination Host Unreachable!

Destination Host Unreachable!

Destination Host Unreachable!

Ping statistics for 192.168.0.1:

Packets: Sent = 4 , Received = 0 , Lost = 4 (100% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms , Maximum = 0ms , Average = 0ms

图14-9 Ping 检测

条目介绍：

➢ **Ping 检测**

目标 IP 地址：	填写需要测试的目标节点的 IP 地址。
发送次数：	填写 Ping 检测时发送的检测包次数。建议使用缺省值。
发送报文长度：	填写 Ping 检测时发送的检测包长度。建议使用缺省值。
时间间隔：	发送 ICMP 请求报文的时间间隔。

14.4.2 Tracert检测

Tracert 检测可以查看交换机到目标节点所经过的路由器。当网络出现故障时，使用该命令可以分析出现故障的网络节点。

在 IP 数据包首部中包含一个 TTL 字段，当数据包在网络中转发时，每经过一个路由 TTL 字段的值减 1。当接收的 IP 数据包的 TTL 字段为 0 或 1 时，路由器将此数据包丢弃，并给发送源回复一个 ICMP 超时报文。这样能有效防止数据包在网络发生故障时，无休止地在网络中流动。

Tracert 检测过程如下：

1) 交换机发送一个 TTL 为 1 的报文给目的设备；
2) 第一跳（即该报文所到达的第一个路由器）回应一个 TTL 超时的 ICMP 报文（该报文中含有第一跳的 IP 地址），这样交换机就得到了第一个路由器的地址；
3) 交换机重新发送一个 TTL 为 2 的报文给目的设备；
4) 第二跳回应一个 TTL 超时的 ICMP 报文，这样交换机就得到了第二个路由器的地址；
5) 重复以上过程直到最终到达目的设备，交换机就得到了从它到目的设备所经过的所有路由器的地址。

进入页面的方法：系统维护>>网络诊断>>**Tracert** 检测

Tracert检测

目标IP： 192.168.0.100 Tracert

最大跳数： 4 跳（1-30） 帮助

Tracert结果

图14-10 Tracert 检测

条目介绍：

➢ **Tracert** 检测

目标 IP：	填写目的设备的 IP 地址。
最大跳数：	填写测试报文发送的最大跳数。

回目录

第15章 软件系统维护

在本交换机中，可以通过FTP功能加载软件。FTP（File Transfer Protocol，文件传输协议）在TCP/IP协议族中属于应用层协议，主要用于在远端服务器和本地主机之间传输文件，是IP网络上传输文件的通用协议。当交换机软件出故障导致无法正常启动时，也可以采用FTP功能重新加载软件。

15.1 硬件连接图

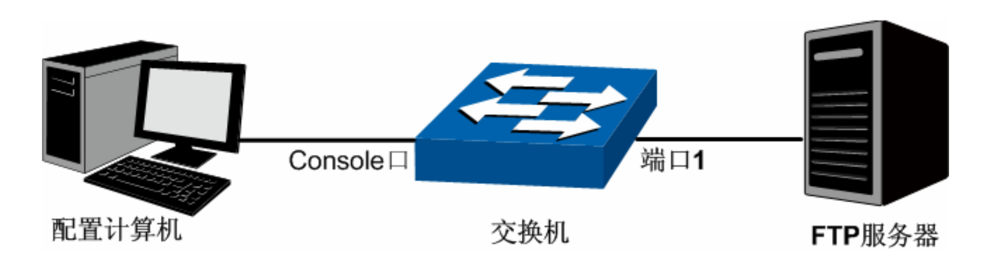


图15-1 利用 FTP 加载软件连接图

1. FTP 服务器通过端口 1 连接到交换机。
2. 配置计算机通过 Console 口与交换机连接。配置计算机和 FTP 服务器可以是同一台主机。
3. 将交换机软件存储在 FTP 服务器的共享目录下，并记录相应用户名、密码以及交换机软件名称，以便后续使用。

15.2 配置超级终端

完成硬件连接后，请按照下面步骤配置管理计算机的超级终端，以便管理交换机。

1. 选择**开始>>所有程序>>附件>>通讯>>超级终端**，打开超级终端。

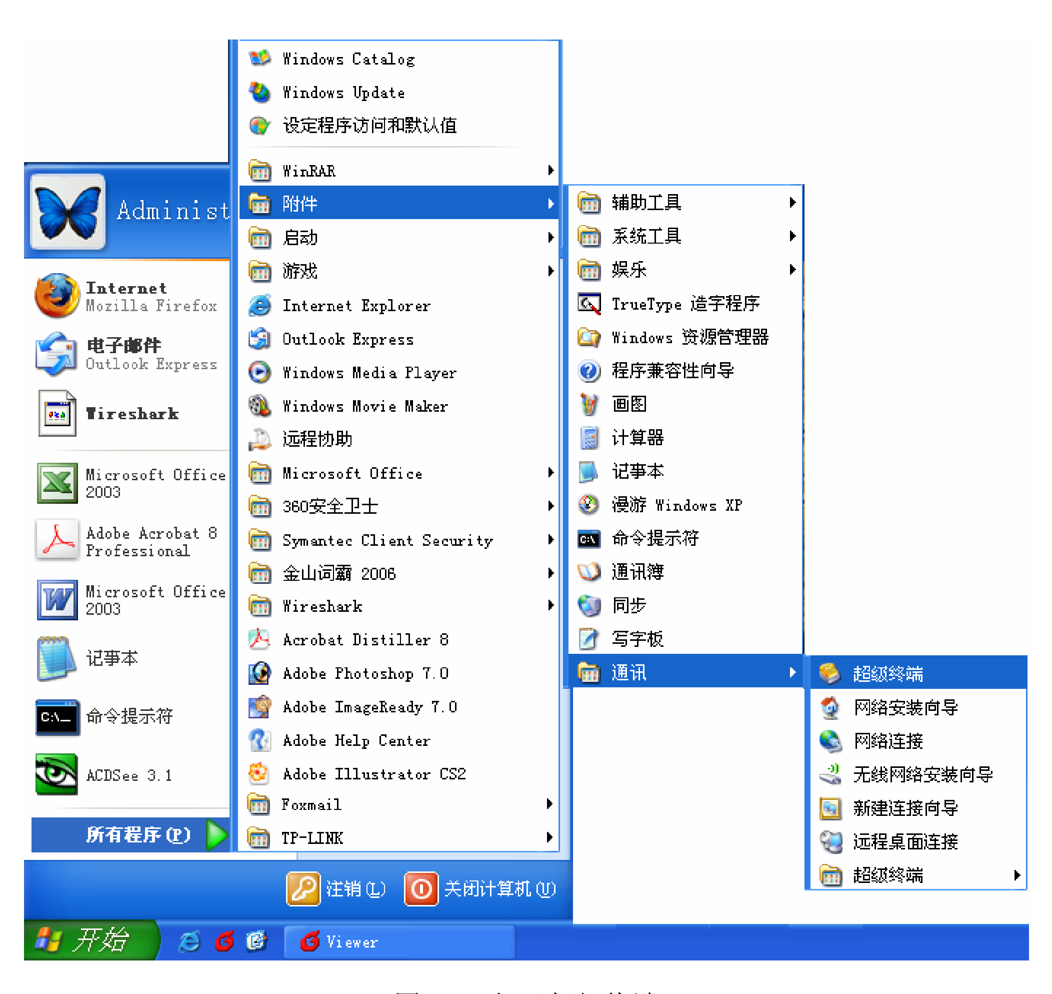


图15-2 打开超级终端

2. 弹出如图15-3所示的连接描述窗口，在名称处键入一个名称，点击**确定**。



图15-3 连接描述

3. 在图15-4中选择连接串口，点击**确定**。



图15-4 连接端口选择

4. 在图15-5中对端口进行参数设置：每秒位数“38400”，数据位“8”，奇偶校验“无”，停止位“1”，数据流控制“无”，然后点击**确定**即可。



图15-5 端口属性设置

15.3 bootrom菜单下加载软件

利用 FTP 功能加载软件需要进入交换机的 bootrom 菜单。请按照下面提示步骤进行操作：

1. 将配置计算机的串口连接到交换机的 Console 口，并打开配置成功的超级终端。FTP 服务器连接到交换机端口 1。
2. 将交换机断电重启，当在超级终端界面中看到提示信息Press CTRL-B to enter the bootrom时，同时按下Ctrl按键和b字母按键进入bootrom菜单，如图15-6所示。

```
*******************************************
*            TP-LINK  BOOTROM             *
*******************************************
Copyright (c) 2009 TP-LINK Tech. Co., Ltd

Press CTRL-B to enter the bootrom
@Bootrom command list:
 help                    - print this list
 reboot                  - reboot the system
 ifconfig                - config the interface
 ftp                     - config the remote host ip,the user name,user password
 and the image file name
 upgrade                 - upgrade the firmware
 start                   - start the system
 reset                   - reset the system to the factory config.
```

图15-6 bootrom 菜单

由于该提示信息显示时间较短，可以在交换机上电后一直按住 Ctrl 按键和 b 字母按键不放，直到进入 bootrom 菜单。

3. 进入 bootrom 菜单后，首先配置交换机的 IP 参数，命令格式为：

   ifconfig ip xxx.xxx.xxx.xxx **mask** 255.255.255.0 **gateway** xxx.xxx.xxx.xxx。

   此处设置交换机的 IP 地址为 172.31.70.22，掩码为 255.255.255.0，网关设置为 172.31.70.1。详细命令如下图所示。输入命令后按回车键。

```
[TP-LINK]: ifconfig ip 172.31.70.22 mask 255.255.255.0 gateway 172.31.70.1
```

4. 然后配置存放升级软件的 FTP 服务器的参数，以方便交换机从 FTP 服务器上下载软件。命令格式为：**ftp host** xxx.xxx.xxx.xxx **user** xxxxx **pwd** xxxxx **file** xxxxxx.bin。

   此处以下面的 FTP 服务器参数为例：IP 地址为 172.31.70.146，登录 FTP 服务器的用户名和密码分别为 123，交换机的升级软件名称为 tl_sl5428_up.bin。详细命令如下图所示。输入命令后按回车键。

```
[TP-LINK]: ftp host 172.31.70.146 user 123 pwd 123 file tl_sl5428_up.bin
```

5. 最后输入 upgrade 命令后按回车键开始升级。等待片刻，超级终端会显示提示信息：You can only use the port 1 to upgrade，如下图所示。请通过交换机的端口 1 连接的 FTP 服务器，若 FTP 没有连接到端口 1 将无法加载软件。请将 FTP 服务器通过端口 1 与交换机连接并重复上述操作。

```
[TP-LINK]: upgrade
You can only use the port 1 to upgrade.
```

6. 当超级终端弹出提示信息：Are you want to upgrade the firmware[Y/N]: 时，输入 Y 开始升级，输入 N 退出升级。如下图所示。图中的#字符表示正在升级，升级结束后将弹出[TP-LINK]命令提示符。

```
Are you want to upgrade the firmware[Y/N]:y
##############################################################################
##############################################################################
##############################################################################
##############################################################################
##############################################################################
#######################################
[TP-LINK]:
```

7. 完成第 6 步后，输入 start 命令启动交换机，如下图所示。出现图示界面后输入用户名和密码（缺省均为“admin”）即可登录交换机的 CLI 命令窗口，可以通过 CLI 命令管理交换机。

```
[TP-LINK]: start
Start..........
◄

****************** User Access Login *********************

User:
```

8. 当忘记了登录交换机的用户名和密码时，可在第 2 步进入交换机 bootrom 菜单后输入 reset 命令来软件复位，复位后恢复到出厂默认设置，登录交换机的用户名和密码均为 admin。

回目录

附录A 802.1X客户端软件使用说明

在 802.1X 体系结构中，客户端作为接入设备需要安装相应的客户端软件，且软件遵循 802.1X 协议标准才能够顺利通过认证。当使用本交换机进行认证时，请使用我司提供的客户端软件进行认证。

1. 安装说明

1. 将光盘放入计算机光驱，在光盘文件夹中，双击安装软件图标，弹出安装语言选择对话框，如下图 1 所示。

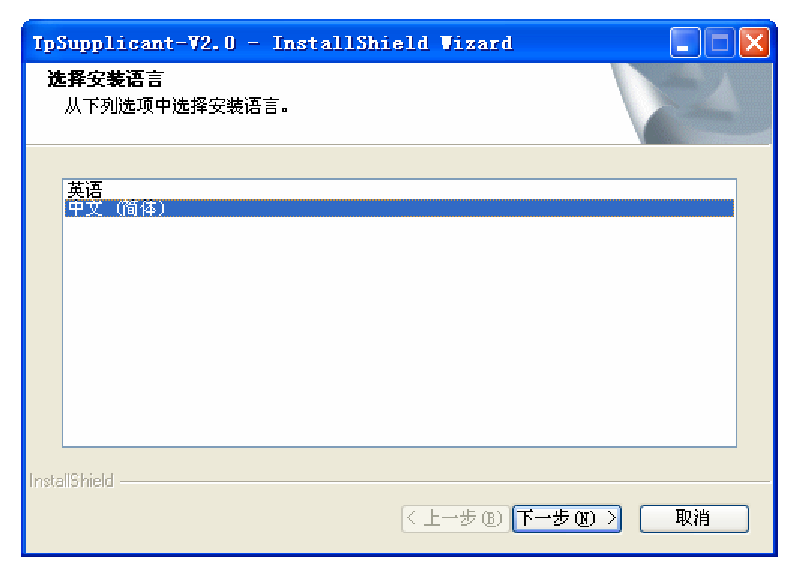


图 1 选择安装语言对话框

2. 单击下一步进入安装准备过程，如下图 2 所示：

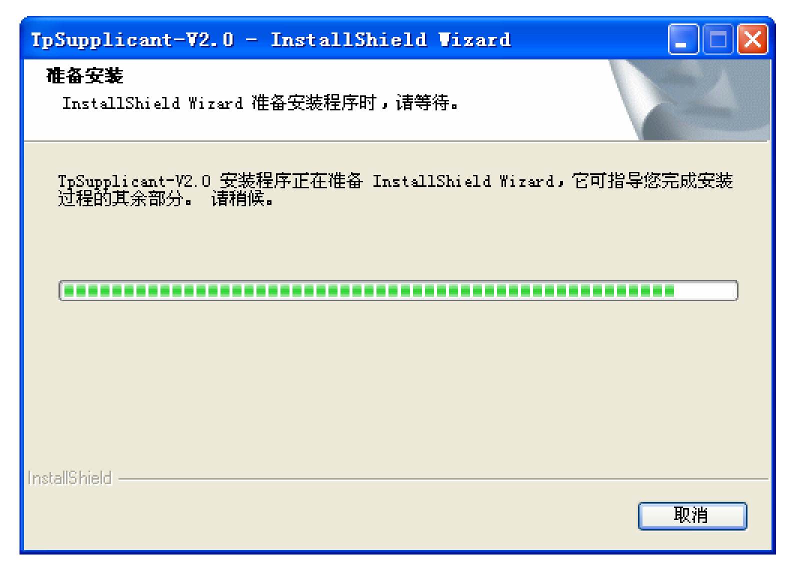


图 2 准备安装对话框

3. 等待片刻，系统准备工作完成后，将自动弹出欢迎对话框，如下图 3 所示，此时可点击<取消>终止安装过程：

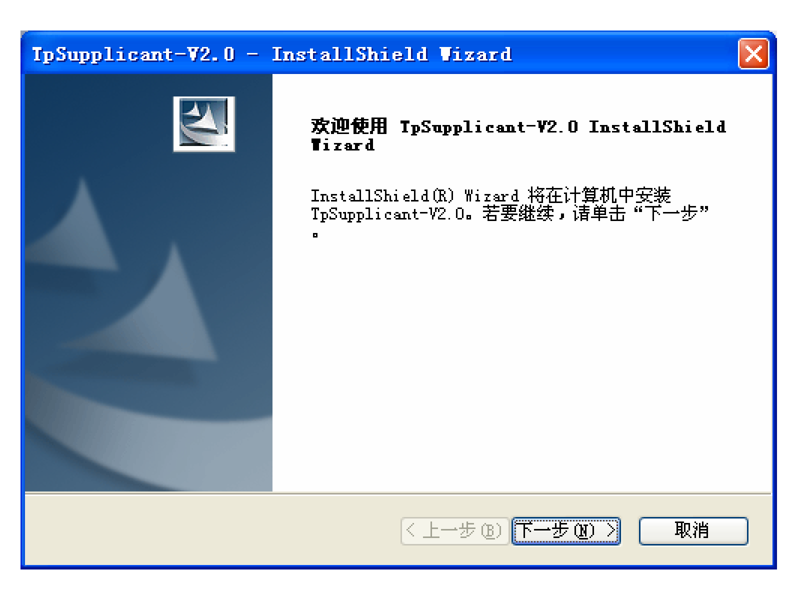


图 3 欢迎对话框

4. 点击<下一步>进行安装路径的选择。如下图 4 所示：

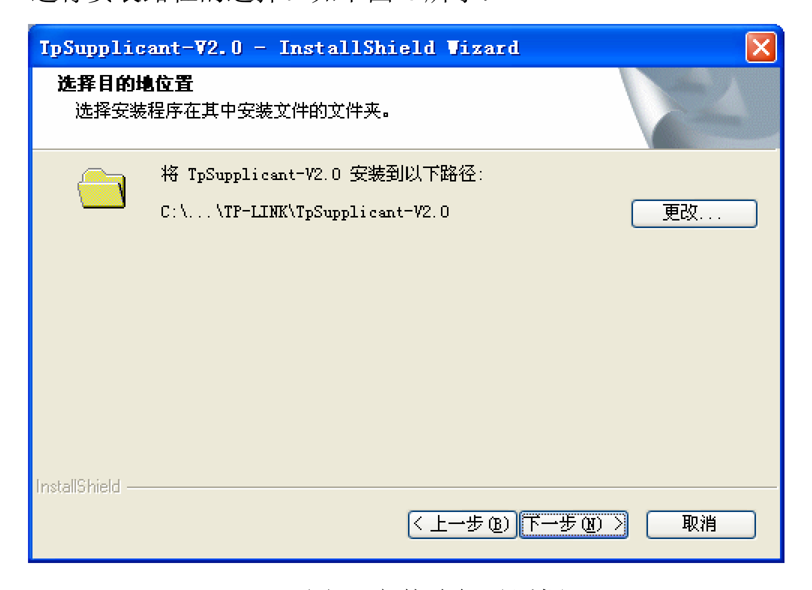


图 4 安装路径对话框

默认路径是系统目录下的 Program Files 目录，点击<更改…>可以选择合适的安装路径。

5. 至此，安装所需参数已确定。点击<下一步>，弹出安装对话框。如下图 5 所示：

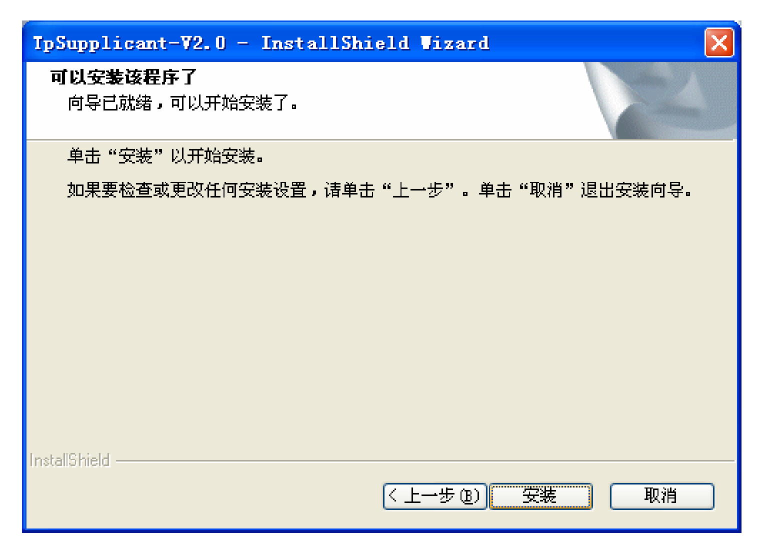


图 5 正在安装

6. 点击<安装>，开始安装 802.1X 客户端软件，如下图 6 所示：

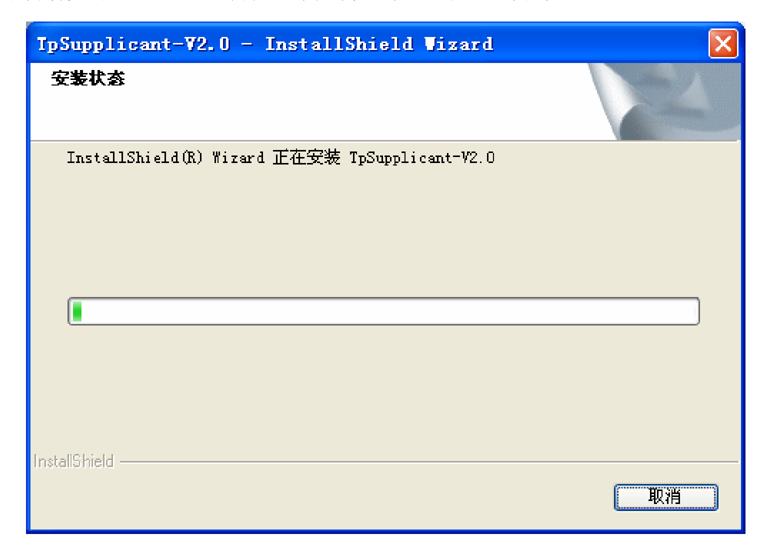


图 6 安装过程

7. 等待片刻，将弹出安装完成对话框。如下图 7 所示：



图 7 安装完成对话框

8. 根据页面提示，安装完成后，如果计算机上没有安装 WinPcap 4.0.2 版本以上的软件，将无法使用该 802.1X 客户端进行认证。请在网上下载 WinPcap 软件并安装。点击<完成>退出。

2. 卸载说明

当需要卸载 TpSupplicant 软件时，可以按照下面步骤执行：

1. 选择：开始 **>>** 所有程序 **>> TP-LINK >> TpSupplicant-V2.0 >>** 卸载 **802.1X** 客户端进行客户端软件卸载。软件卸载准备对话框如下图 8 所示：

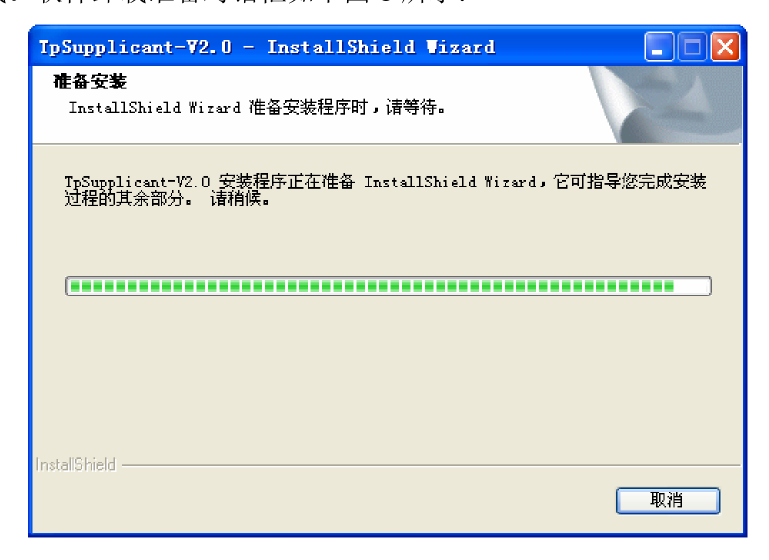


图 8 软件卸载准备

2. 点击<是>，开始卸载软件，如下图 9 所示：

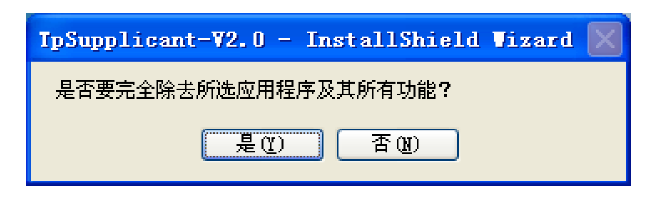


图 9 卸载软件

3. 卸载结束后，点击<完成>关闭窗口即可，如下图 10 所示：

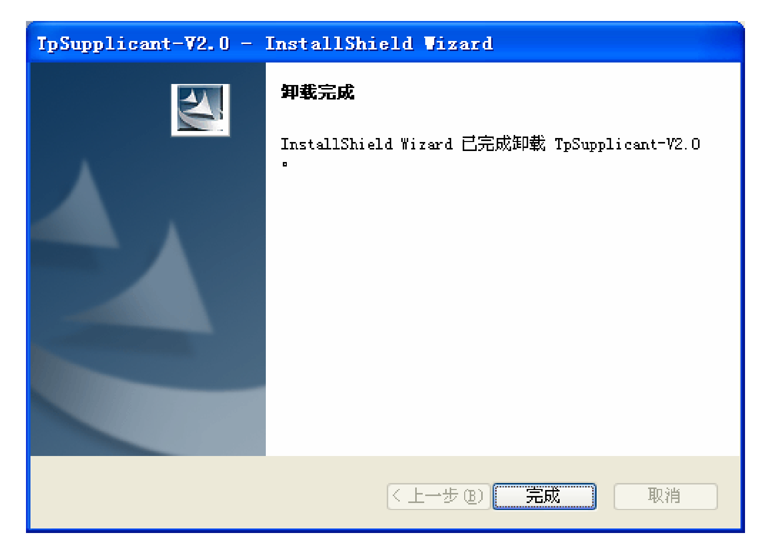


图 10 完成卸载

3. 使用说明

1. 安装完成后，双击桌面 TP-LINK 802.1X 客户端软件图标运行应用程序，弹出程序主对话框如下图 11 所示：



图 11 主对话框

在用户名和密码中输入服务器端设定好的用户名和密码，注意用户名和密码均不得多于 15 个字符。

2. 点击<属性>按键，弹出属性对话框，可以对拨号属性进行适当的设置，如下图 12 所示：

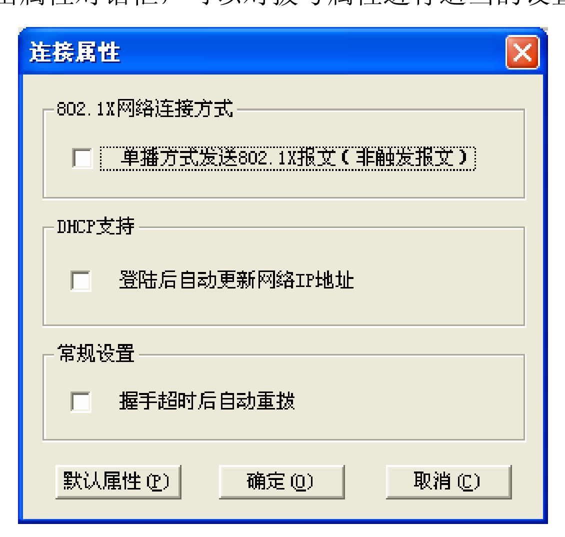


图 12 属性对话框

单播方式发送 802.1X 报文（非触发报文）：选择此项时，客户端将以组播的方式向交换机申请认证，然后以单播方式发送认证报文。

登陆后自动更新 IP 地址：如果接入网络中设置了 DHCP 服务器为客户端分配 IP，请选择此项功能。认证成功后 DHCP 服务器会自动给客户端分配 IP 地址，客户端获得新的 IP 地址后才能访问网络。

握手超时后自动重拨：选择此项时，如果客户端在一定的时间内没有收到交换机的握手应答报文，则说明客户端和交换机的连接可能出现问题，这时客户端软件将自动重新发起连接。

3. 在主窗口如图 11 界面下如果点击<连接>，将弹出认证状态对话框显示认证过程，如下图 13 所示：

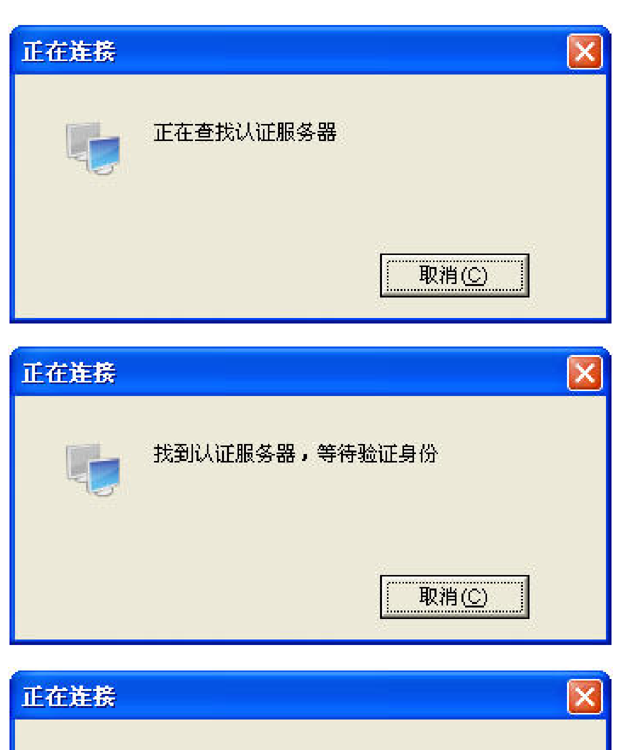




图 13 认证状态对话框

4. 当顺利的通过认证后，会显示一个认证通过对话框，如下图 14 所示：



图 14 认证通过对话框

5. 双击系统托盘中的连接状态图标，将弹出连接状态对话框，如下图 15 所示：



图 15 连接状态对话框

4. 常见问题：

1. 运行该软件的时出现如下图所示的错误对话框时如何处理？



图 16 缺失 DLL 对话框

答：如果出现图 16 对话框，说明缺少了支持的 DLL 文件，如果没有安装 WinPcap 4.0.2 或以上版本，请先到 http://www.winpcap.org 下载安装最新版本 WinPcap 软件，然后重新运行该客户端。

2. 可以使用该软件拨号其它公司生产的交换机吗？

答：不可以，该软件是专门为我司交换机定制。

3. 如果我设置保存密码会不会不安全？

答：不会，保存到配置文件中的密码已经经过加密。

回目录

附录B 术语表

【 # A B C D E F G H I J L M N O P Q R S T U V W 】

英文缩写	英文全称	中文全称
A		回首页
AAA	Authentication, Authorization and Accounting	认证、授权和计费
ACL	Access Control List	访问控制列表
ARP	Address Resolution Protocol	地址解析协议
-	Auto-Negotiation	自协商
B		回首页
BOOTP	Bootstrap Protocol	自举协议
BPDU	Bridge Protocol Data Unit	网桥协议数据单元
-	Broadcast Storm	广播风暴
-	Broadcast	广播
-	Broadcast Domain	广播域
C		回首页
CFI	Canonical Format Indicator	标准格式指示位
CHAP	Challenge Handshake Authentication Protocol	质询握手验证协议
CIST	Common and Internal Spanning Tree	公共和内部生成树
CMP	Cluster Management Protocol	集群管理协议
CRC	Cyclic Redundancy Check	循环冗余校验
CoS	Class of Service	服务等级
CSMA/CD	Carrier Sense Multiple Access/Collision Detect	载波侦听多路访问/冲突检测
CST	Common Spanning Tree	公共生成树
D		回首页
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
-	DHCP Client	DHCP 客户端
DNS	Domain Name System	域名系统
DoS	Denial of Service	拒绝服务
DSCP	Differentiated Services Code Point	差分服务编码点
E		回首页
EAP	Extensible Authentication Protocol	可扩展认证协议

英文缩写	英文全称	中文全称
EAPOL	Extensible Authentication Protocol over LAN	局域网上的可扩展认证协议
EAPOR	EAP over RADIUS	承载于 RADIUS 协议的 EAP
-	Ethernet	以太网
F		回首页
FE	Fast Ethernet	快速以太网
FDB	Forward Data Base	地址表
-	Flow Control	流控
-	Frame	帧
FTP	File Transfer Protocol	文件传输协议
-	Full-Duplex	全双工
G		回首页
GARP	General Attributes Registration Protocol	通用属性注册协议
GBIC	Giga Bitrate Interface Converter	千兆接口转换器
GE	Gigabit Ethernet	千兆以太网
GVRP	GARP VLAN Registration Protocol	GARP VLAN 注册协议
H		回首页
-	Half-Duplex	半双工
HTTP	Hyper Text Transport Protocol	超级文本传送协议
HTTPS	Secure Hyper Text Transfer Protocol	安全超文本传输协议
I		回首页
IANA	Internet Assigned Numbers Authority	因特网编号授权委员会
ICMP	Internet Control Message Protocol	因特网控制报文协议
IEEE	Institute of Electrical and Electronics Engineers	电机工程师协会
IETF	Internet Engineering Task Force	因特网工程任务组
IGMP	Internet Group Management Protocol	互联网组管理协议
-	IGMP-Snooping	互联网组管理协议窥探
IP	Internet Protocol	互联网协议、网际协议
-	IP Address	IP 地址
-	IP Multicast	IP 组播
ISO	International Organization for Standardization	国际标准化组织
ISP	Internet service provider	因特网服务提供商
IST	Internal Spanning Tree	内部生成树
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector	国际电信联盟-电信标准部
J		回首页

英文缩写	英文全称	中文全称
-	Jumbo Frame	超长帧
L		回首页
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
LACP	Link Aggregation Control Protocol	链路聚合控制协议
LACPDU	Link Aggregation Control Protocol Data Unit	链路聚合控制协议数据单元
LAG	Link Aggregated Group	链路聚合组
LAN	Local Area Network	局域网
LCP	Link Control Protocol	链路控制协议
M		回首页
MAC	Media Access Control	媒体访问控制
MAPT	Network Address Port Translation	网络地址端口转换
MIB	Management Information Base	管理信息库
MODEM	MOdulator-DEModulator	调制解调器
MSTI	Multi-Spanning Tree Instance	多生成树实例
MSTP	Multiple Spanning Tree Protocol	多生成树协议
MTU	Maximum Transmission Unit	最大传输单元
-	Multicast	组播
N		回首页
NAPT	Network Address Port Translation	网络地址端口转换
NAT	Net Address Translation	网络地址转换
NDP	Neighbor Discovery Protocol	邻居发现协议
NMS	Network Management Station	网络管理站
NPDU	Network Protocol Data Unit	网络协议数据单元
NTDP	Neighbor Topology Discovery Protocol	邻居拓扑发现协议
NTP	Network Time Protocol	网络时间协议
-	NTP Server	网络时间服务器
O		回首页
OID	Object Identifier	对象标识符
OSI	Open Systems Interconnection	开放系统互连
OSPF	Open Shortest Path First	开放最短路径优先
OUI	Organizationally Unique Identifier	全球统一标识符
P		回首页
P2P	Point To Point	点到点
-	Packet	数据包

英文缩写	英文全称	中文全称
PAP	Password Authentication Protocol	密码认证协议
PCB	Printed Circuit Board	印制电路板
PDU	Protocol Data Unit	协议数据单元
PING	Packet Internet Groper	Internet 包探测器
PoE	Power over Ethernet	以太网供电
-	Port	端口
PPP	Point-to-Point Protocol	点到点协议
PPTP	Point to Point Tunneling Protocol	点对点隧道协议
PQ	Priority Queuing	优先队列
Q		回首页
QoS	Quality of Service	服务质量
-	Query	查询
R		回首页
RADIUS	Remote Authentication Dial in User Service	远程认证拨号用户服务
RIP	Routing Information Protocol	路由信息协议
RMON	Remote Monitoring	远程网络监视
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
-	Router	路由器
S		回首页
-	Server	服务器
SFTP	Secure FTP	安全文件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SP	Strict Priority Queuing	严格优先级队列
SPF	Shortest Path First	最短路径优先
SSH	Secure Shell	安全外壳
SSL	Secure Sockets Layer	加密套接字协议层
STP	Spanning Tree Protocol	生成树协议
-	Switch	交换机
T		回首页
TCP	Transmission Control Protocol	传输控制协议
-	Telnet	远程登录
TFTP	Trivial File Transfer Protocol	简单文件传输协议
ToS	Type of Service	服务类型
TPID	Tag Protocol Identifier	标签协议标识符

英文缩写	英文全称	中文全称
TRIP	Trigger RIP	触发路由信息协议
TTL	Time to Live	生存时间
-	Trap	陷阱
U		回首页
UDP	User Datagram Protocol	用户数据包协议
-	Unicast	单播
URL	Uniform Resource Locators	统一资源定位
USM	User-Based Security Model	基于用户的安全模型
UTP	Unshielded Twisted Pair	非屏蔽双绞线
V		回首页
VACM	View-based Access Control Model	基于视图的访问控制模型
VLAN	Virtual Local Area Network	虚拟局域网
VOS	Virtual Operate System	虚拟操作系统
W		回首页
WAN	Wide Area Network	广域网
WLAN	wireless local area network	无线局域网
WRR	Weighted Round Robin Queuing	加权轮询队列
WWW	World Wide Web	万维网

回目录

附录C 技术参数规格

参数项	参数内容
支持的标准和协议	IEEE 802.3 10BASE-T 以太网 IEEE 802.3u 100BASE-TX 快速以太网 IEEE 802.3ab 1000BASE-T 千兆以太网 IEEE 802.3z 千兆以太网(光纤) ANSI/IEEE 802.3 N-Way 自动协商 IEEE 802.3x 流量控制 IEEE 802.1p 优先级 IEEE 802.1q VLAN 桥操作 IEEE 802.1X 基于端口的访问认证 CSMA/CD Ethernet
数据传输速率	以太网 10Mbps 半双工，20Mbps 全双工 快速以太网 100Mbps 半双工，200Mbps 全双工 千兆以太网 2000Mbps 全双工
网络介质	10BASE-T： 3 类或以上 UTP/STP(≤100m) 100BASE-TX： 5 类或以上 UTP/STP(≤100m) 1000Base-T： 4 对 5 类(推荐超 5 类)UTP/STP(≤100m)
指示灯	PWR、SYS、10/100M 指示灯、1000M 指示灯
传输方式	存储转发
背板带宽	12.8Gbps
MAC 地址学习	自动更新，支持 8K 地址空间
包转发速率	10BASE-T：14881pps/端口 100BASE-TX：148810pps/端口 1000Base-T：1488095pps/端口
交流输入	100-240V~ 50/60Hz
工作温度	0℃~40℃
存储温度	-40℃~70℃
湿度	5%~90%（RH 无凝结）
尺寸（长×宽×高）	440mm×260mm×44mm

回目录